

TRABAJO FIN DE GRADO GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

FACULTAD DE ECONOMÍA Y EMPRESA.
UNIVERSIDAD DE SALAMANCA.

CURSO ACADÉMICO: 2020/2021

ANÁLISIS ECONÓMICO DE CRIPTOACTIVOS Y TECNOLOGÍA BLOCKCHAIN



AUTOR : LUIS ROMO CONDE
TUTOR: PROF. DR. JOSÉ DAVID VICENTE LORENTE



ECONOMIC ANALYSIS OF CRYPTOASSETS AND BLOCKCHAIN TECHNOLOGY

AUTOR: LUIS ROMO CONDE

**TUTOR: PROF. DR. JOSÉ
DAVID VICENTE LORENTE**

RESUMEN

El sistema de compraventa, el mercado financiero -en especial el de las inversiones- y los medios de pago coexistentes al hombre, han visto evolucionar sus características y fundamentos en virtud de las necesidades y realidades de cada época.

El objetivo principal de este trabajo, como es sencillamente deducible del propio título, es tratar de aportar un análisis sobre el amplio mundo de los 'criptoactivos' ('criptomonedas' o 'criptodivisas') y de la tecnología Blockchain. Ubicando el mismo no sólo en una verdad práctica sino también en una realidad teórica, se pretende proveer de las herramientas más elementales para su examen y conocimiento. De esta manera, acercar al lector a la evolución, características, procedencia, datos y estadísticas, que ambos conceptos llevan aparejados a su ADN.

Por último, la exposición comparativa de las principales 'criptomonedas' y sus datos más relevantes, busca proporcionar el sustento para que cada uno de los interesados pueda analizar y sacar sus propias conclusiones personales en base a ellos, e incluso frente al mercado bursátil -como también se facilita-, intentando dotar en todo momento al trabajo de una objetividad máxima.

PALABRAS CLAVE: Inversiones. Medios de Pago. Criptoactivos. Tecnología Blockchain. Verdad Práctica. Realidad Teórica.

ABSTRACT

The trading system, the financial market -especially the investments- and the means of payment coexisting with mankind, have seen their characteristics and foundations evolve according to the needs and realities of each era.

The main objective of this work, as can simply be deduced from the title itself, is to provide an analysis of the great world of cryptoassets ('cryptocurrencies') and Blockchain technology. Placing it not only in a practical truth but also in a theoretical reality, it provides the most elementary tools for its analysis and knowledge. In this way, the aim is to bring the reader closer to the evolution, characteristics, origin, data and statistics that both concepts have in their DNA.

Finally, the comparative exposition of the main 'cryptocurrencies' and their most relevant data, seeks to provide the support so that each of the interested parties to analyse and draw their own personal conclusions based on them, and even against the stock market -as it is also provided-, trying to provide this work with maximum objectivity at all times.

KEYWORDS: Investments. Means of payment. Cryptoassets. Blockchain technology. Practical Truth. Theoretical Reality.

ÍNDICE

1. INTRODUCCIÓN.....	6
2. LA TECNOLOGÍA BLOCKCHAIN.....	8
2.1. Historia del dinero y contextualización de la tecnología Blockchain.....	8
2.2. Características, funciones y limitaciones de la moneda fiduciaria.....	12
2.3. Paper de Nakamoto.....	13
2.4. <i>Distributed Ledger Technology</i> (DLT).....	15
2.5. Funcionamiento de la tecnología Blockchain.....	17
2.6. Diferentes tipologías en la realidad práctica de la tecnología Blockchain..	19
2.6.1. <i>Blockchain pública</i>	20
2.6.2. <i>Blockchain privada</i>	21
2.6.3. <i>Blockchain federal o de consorcio</i>	22
2.6.4. <i>Síntesis comparativa entre los tres tipos generales de tecnología Blockchain</i>	22
3. CRIPTOACTIVOS / CRIPTOMONEDAS / CRIPTODIVISAS.....	23
3.1. ¿Qué es un criptoactivo? Orígenes y nociones fundamentales.....	23
3.2. Los criptoactivos en la actualidad.....	24
3.3. Tipos de criptoactivos. Principales referentes en el mercado.....	25
3.3.1. <i>Bitcoin (BTC)</i>	25
3.3.1.1. <i>Evolución histórica del precio de BTC</i>	27
3.3.2. <i>Ethereum (ETH)</i>	27
3.3.2.1 <i>Evolución histórica del precio de ETH</i>	28
3.3.3. <i>Tether (USDT)</i>	28
3.3.3.1 <i>Evolución histórica del precio de USDT</i>	30
3.3.4. <i>Binance Coin (BNB)</i>	30
3.3.4.1. <i>Evolución histórica del precio de BNB</i>	32
3.3.5. <i>Cardano (ADA)</i>	32
3.3.5.1. <i>Evolución histórica del precio de ADA</i>	33

4. ANÁLISIS COMPARATIVO DE REFERENCIAS DEL MERCADO DE CRIPTOACTIVOS.....	34
4.1. Principales valores de las criptomonedas estudiadas: BTC, ETH, USDT, BNB y ADA.....	34
4.2. Variación porcentual en el precio de las criptomonedas estudiadas (BTC; ETH; USDT; BNB; ADA) con respecto a los índices bursátiles S&P 500 e IBEX 35 en los últimos 5 años.....	35
4.2.1. <i>Exposición gráfica conjunta de las variaciones recogidas en apartado 4.2</i>	35
4.3. Ranking global de las 10 criptomonedas con mayor valor en el mercado actual.....	37
4.4. Ranking global de las 10 criptomonedas con mayor volumen de negociación en el mercado actual.....	37
4.5. Clasificación de los 10 países a nivel mundial con mayor demanda de sus ciudadanos en el mercado de las criptomonedas.....	38
5. CONCLUSIONES.....	39
6. BIBLIOGRAFÍA.....	41

ÍNDICE DE TABLAS, CUADROS, FIGURAS Y GRÁFICOS

SECCIÓN 2. LA TECNOLOGÍA BLOCKCHAIN

Tabla 2.1. Síntesis comparativa de los tres tipos de tecnología Blockchain (p. 22).

SECCIÓN 3. CRIPTOACTIVOS / CRIPTOMONEDAS / CRIPTODIVISAS

Gráfica 3.1. Evolución histórica del precio de BTC (p. 27).

Gráfica 3.2. Evolución histórica del precio de ETH (p. 28).

Gráfica 3.3. Evolución histórica del precio de USDT (p. 30).

Gráfica 3.4. Evolución histórica del precio de BNB (p. 32).

Gráfica 3.5. Evolución histórica del precio de ADA (p. 33).

SECCIÓN 4. ANÁLISIS COMPARATIVO DE REFERENCIAS DEL MERCADO DE CRIPTOACTIVOS.

Tabla 4.1. Análisis comparativo de los principales valores y referencias en el mercado (p. 34).

Tabla 4.2. Análisis comparativo de la variación porcentual en el precio de las criptomonedas estudiadas (BTC; ETH; USDT; BNB; ADA) con respecto a los índices bursátiles S&P 500 e IBEX 35 en los últimos 5 años (p. 35).

Gráfica 4.3. Exposición gráfica conjunta de las variaciones recogidas en la tabla 3.7., a excepción de la correspondiente a ETH (p. 36).

Gráfica 4.4. Exposición gráfica individual de las variaciones de ETH recogidas en la tabla 3.7. (p.36).

Tabla 4.5. Ranking global de las 10 criptomonedas con mayor valor en el mercado actual (p.37).

Tabla 4.6. Ranking global de las 10 criptomonedas con mayor volumen de negociación en el mercado actual (p.37).

Gráfica 4.7. Clasificación de los 10 países a nivel mundial con mayor demanda de sus ciudadanos en el mercado de las criptomonedas (p.38).

1. INTRODUCCIÓN

La digitalización de la realidad global, y con ello la de ‘nuestras vidas’, es un hecho que influye en (casi) todos los ámbitos, decisiones y actuaciones que realizamos. Y aún más lo será en un futuro más cercano que lejano.

El mundo de las finanzas no se ha quedado al margen de las tecnologías y del ‘boom’ e impacto total que ha suscitado en la sociedad la tecnología Blockchain, y con ella el nacimiento de la moda digital Bitcoin, abriendo el camino de la revolución monetaria en términos tecnológicos. De esta manera, en el año 2008 de la mano de ‘Satoshi Nakamoto’ se inició la revolución global en la manera de concebir y practicar la transmisión de valor y la inversión financiera. El desconocimiento de mucha gente choca de lleno con el atrevimiento y la confianza depositada por otros muchos en la figura inicial del sistema Bitcoin, y de las criptomonedas sucesivas que han ido ‘naciendo’ desde comienzos de la década. Esta realidad ha logrado, prácticamente a partes iguales, tanto apoyo como rechazo institucional y empresarial a nivel mundial, manifestándose así la concepción contradictoria y las diversas opiniones vertidas sobre esta nueva realidad.

En este marco, pero sin entrar a valorar y reflejar ningún tipo de discusión pública o doctrinal, el trabajo trata de exponer -de la manera más objetiva y a la vez más llana posible- el escenario de la tecnología Blockchain y de las criptomonedas. Teniendo en cuenta dicho objetivo, y tratando de aportar al lector un trabajo accesible en su explicación e interesante en su contenido, el mismo se encuentra estructurado en 6 apartados, distribuidos de la siguiente manera:

- El punto 1 se corresponde con la introducción del trabajo, destacándose -tanto en la versión en castellano como en inglés (‘abstract’)- 6 palabras claves.
- El punto 2 (*La tecnología Blockchain*) contiene una exposición inicial de la tecnología Blockchain -soporte digital y existencial para el correcto funcionamiento y validez de las criptovidasas- tratando su origen, contextualizando su presencia en la historia del dinero; sus características, funciones,

- funcionamiento y limitaciones; abordando en último lugar los diferentes tipos de la misma. Además, se desarrolla el *paper* de ‘Satoshi Nakamoto’ y la tecnología DLT.
- El punto 3 (*Criptoactivos/Criptomonedas/Criptodivisas*) centra su investigación en la realidad general de los criptoactivos (nacimiento, características, tipos y referentes), ahondado en el funcionamiento, peculiaridades y análisis de los 5 más relevantes (Bitcoin, Ethereum, Tether, Binance Coin y Cardano).
 - El punto 4 (*Análisis comparativo de referencias del mercado de criptoactivos*) recoge el estudio de las principales referencias estadísticas de las 5 criptomonedas desarrolladas en el punto anterior, facilitando para ello una tabla comparativa entre todas ellas. Posteriormente, se muestran una tabla y una gráfica realizadas en base a la variación porcentual de la evolución del precio de estas en los últimos 5 años, junto con la de los índices bursátiles S&P 500 e IBEX 35. Además, se incorporan 2 rankings globales de las criptodivisas con mayor valor y volumen de negociación, y una gráfica final explicativa de los 10 países donde el papel de las criptomonedas es mayor.
 - En último lugar, los puntos 5 y 6 están dedicados respectivamente a las conclusiones personales del autor del trabajo y a la bibliografía empleada en la elaboración del mismo.

En consecuencia, durante toda la investigación y exposición posterior, se ha tratado esencialmente de aportar una doble vertiente al tema de fondo: “*Análisis económico de los criptoactivos y de la tecnología Blockchain*”. Primeramente, una vertiente teórica necesaria para el conocimiento de una realidad tan extensa, con la que poder entender y comprender la realidad; y otra posterior, con mayores tintes prácticos, basada y completada con el estudio estadístico de diferentes variables y referencias de las criptomonedas “más importantes”, con el objetivo primordial de proporcionar cierta evidencia comparativa sobre la rentabilidad de los criptoactivos frente a opciones de inversión más convencionales. Para ello, se ha recurrido a fuentes bibliográficas de diferente índole: aquellas con las que profundizar en los conceptos más técnicos y teóricos empleados durante el trabajo, enfocándolos desde la perspectiva más clara y simple; otras más prácticas con la pretensión de dotar al mismo de gran contenido

estadístico, gráfico y numérico; diferentes referencias a economistas, autoridades y referentes del mundo financiero, reuniendo sus reflexiones y opiniones sobre la realidad de los criptoactivos. Envuelto todo ello de los conocimientos adquiridos a lo largo de mi experiencia y aprendizaje personal durante el estudio de la *Doble Titulación en Grado de Administración y Dirección de Empresas y en Grado de Derecho* en la *Universidad de Salamanca*, queriendo enriquecer al lector mediante constantes referencias a noticias, artículos de investigación e informativos, revistas y diarios digitales de divulgación, blogs y páginas web, y a trabajos académicos.

2. LA TECNOLOGÍA BLOCKCHAIN

2.1. Historia del dinero y contextualización de la tecnología Blockchain

Desde el origen hasta la actualidad, la existencia del ser humano siempre ha estado acompañada de un mercado comercial o de intercambio, mediante el que poder satisfacer sus necesidades materiales y de servicios.

- Desde el neolítico, el trueque surgió en torno al nacimiento de la sociedad agricultora-ganadera (con anterioridad al año 7000 a.C.). Ese medio primigenio consistía en el intercambio de bienes o servicios de un sujeto con otro¹.
- Posteriormente, en torno al año 600 a.C², emanó el dinero mercancía. Las complicaciones presentadas por el trueque en determinadas transacciones y la caducidad de numerosos recursos, provocó este hecho. Debido a su formalización, se requería que los bienes en cuestión fueran duraderos, divisibles y limitados. Por ello, se recurrió a los metales preciosos para la realización de las monedas, los cuales debían ser examinados sobre su calidad y el grado de pureza, complicándose en ocasiones por la falta efectividad y rapidez del sistema. Gracias a la acuñación de la moneda se eliminó este problema.
- La agilidad del mercado y la incomodidad en el transporte de grandes cantidades de dinero mercancía trajo consigo la aparición del papel moneda y billete. Con

¹ El trueque resultó un sistema deficiente a medida que el mercado ganaba en complejidad, ya que generaba dudas en la valoración de bienes y servicios menos comunes entre los sujetos.

² La fecha de aparición de la moneda está registrada alrededor de los años 680-560 a.C en la actual Turquía.

origen en el siglo VII en China, no fue hasta el año 812 cuando su uso y presencia se instaure oficialmente. Durante el siglo X, la aplicación de esta práctica se extendió por todo el continente, sustituyéndose la emisión que los sujetos poseían en favor exclusivo del Gobierno central. En Europa, fue en 1661 cuando tuvo lugar la primera emisión, gracias al *Banco de Estocolmo* y su práctica de entrega a todos aquellos que mantuvieran metales en la entidad. En el siglo XVIII se extendió por todo el continente europeo. En torno a 1970, se eliminó el sistema “patrón oro”³ en lugar del sistema actual.

- En 1914, de la mano de *Western Union*, nacieron las tarjetas de crédito. En 1958 fueron proporcionadas por las entidades bancarias, dentro de los servicios ofertados. Con posterioridad, la primera de estas se conoció como *VISA*.
- En el año 1970 finalizaron los acuerdos de *Bretton Woods*. Se trataba de una serie de resoluciones acordadas en el seno de la *ONU* en julio de 1944, donde se establecían las reglas comerciales y financieras para el desarrollo de las relaciones mercantiles y comerciales. El fin de los ideales proteccionistas, la consolidación de las políticas librecambistas, la creación del *Banco Mundial* y del *Fondo Monetario Internacional*, la colocación del dólar como moneda mundial de referencia⁴ y la promesa de pago con oro a los bancos el dinero, entre otros, fueron algunas de las medidas recogidas en estos acuerdos. Sin embargo, como consecuencia de la *Guerra de Vietnam* (1955-1975) y la impresión descontrolada de dinero realizado por los Estados Unidos, los principales países mundiales abandonaron el sistema y comenzó el mercado de tipos cambiarios fluctuantes.
- De la mano del surgimiento de Internet, aparece la compra y venta de servicios digitales. *Peapod* fue una de las empresas precursoras en este ámbito, llegando a la realidad actual de las diferentes formas de mercado digital: móvil, ordenador, tablet, relojes inteligentes, entre otros.
- Ahora bien, es en el año 2008 cuando tiene lugar un cambio trascendental en la concepción del mercado: el nacimiento del dinero virtual. Este hecho se produce

³ Los billetes certificados representaban una cantidad de valor que era respaldada por los bancos en su equivalente en oro.

⁴ Cada país respaldaba la emisión gracias al oro que este almacenaba en las arcas nacionales.

con el desarrollo de la *tecnología Blockchain o cadena de bloques*: “base de datos que puede ser compartida por una gran cantidad de usuarios en forma de peer-to-peer y que permite almacenar información de forma inmutable y ordenada. La información ardiada es pública y puede ser consultada en cualquier momento por cualquier usuario de la red” (Dolader, Bel y Muñoz, 2017) dentro del proyecto Bitcoin. La Autoridad Bancaria Europea (2014) definió la moneda virtual como “una representación digital de valor, que no es emitido por un banco central o una autoridad pública, ni necesariamente conectada a un dinero fiduciario, pero que es aceptado por personas naturales o jurídicas como medio de pago y puede ser transferido, almacenado o intercambiado electrónicamente”⁵.

A diferencia del concepto esencial de moneda generalizado en la sociedad, cuando se utiliza para referirse al dinero virtual, se hace con un matiz adicional: a lo largo de la historia, la noción del dinero ha girado en exclusiva en su uso como medio de pago o intercambio, mientras que gracias al dinero digital, el dinero también es utilizado como un bien o activo de inversión. La globalización de nuestros días impregna cada uno de los ámbitos de nuestra realidad. Y la tecnología Blockchain es un ejemplo fiel de este fenómeno propio del siglo XXI.

Cuando el sistema económico se basaba en la caza, en la pesca y en la recolección de frutas y recursos, el hombre comercializaba en un entorno reducido, cercano a su mínima realidad diaria. A medida que la sociedad fue desarrollándose fueron apareciendo diferentes instituciones encargadas de la gestión, creación y distribución del dinero: bancos, empresas y gobiernos. El origen de la banca se remonta a la antigua Mesopotamia, sobre el año 2000 a.C, cuando se hacían préstamos de granos a los mercaderes, ganaderos y comerciantes de la época. Surgieron rutas comerciales, se implantaron las importaciones/exportaciones como forma comercial y con ello, el comercio menor se expandió a una dimensión desconocida hasta entonces. En ese

⁵ Bedecarratz, F. (2018). Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal. *Revista chilena de derecho y tecnología*, 1, 79-105. Recuperado de: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000100079 [2 de junio de 2021].

proceso de desarrollo, el sistema se hizo más complejo, provocando la pérdida de control que, en sus comienzos, cada uno de los sujetos tenía sobre su reducido campo de actividad. En cambio, la idea de banca como tal, debemos situarla en Italia, con familias nobles de finales de la Edad Media y comienzos del Renacimiento, creadoras de importantes y “revolucionarias” entidades bancarias. Juan de Médici dio nombre a uno de los bancos más influyentes e importantes: el Banco Médici. Posteriormente, se fueron abriendo sucursales y la banca se instauró en toda Europa durante los siglos ulteriores. Entre los acontecimientos más importantes, cabe destacar los siguientes:

- 1602: fundación de la *Bolsa de Ámsterdam*, pionera y primera.
- 1656: primer uso del papel-moneda por parte de un banco sueco.
- 1694: fundación del *Banco de Inglaterra*.
- 1720: gran crisis financiera en toda Europa que provocó la “bancarrota” de muchos banqueros del continente.
- 1775: fundación de la primera sociedad en préstamos inmobiliarios.
- 1791: fundación de la primera banca de los Estados Unidos.
- 1800: fundación del *Banco de gracia* por Napoleón Bonaparte.
- 1817: fundación de la bolsa de Nueva York.
- 1818: nacimiento del primer banco de París en materia de ahorros.
- 1857: fundación en España del *Banco de Bilbao* y el *Banco Santander*.
- 1870: fundación del *Deutsche Bank* alemán.
- 1913: nacimiento del *Sistema de Reserva Federal* de los Estados Unidos.
- 1933: cierre de más de 9000 entidades bancarias en el mundo, tras la crisis de Wall Street de 1929 (“Crac del 29”).

El surgimiento de Internet y su implantación en la vida cotidiana a finales del siglo pasado, ha revolucionado, como es patente, la sociedad en todos sus ámbitos. Plataformas de mercado (*Amazon, Ebay, Aliexpress*), instituciones digitalizadas (*Administraciones públicas, universidades, colegios*), plataformas de las entidades bancarias (*Santander, Unicaja, BBVA*), programas digitales (*Citas de sanidad, app rastreo Covid-19*), webs de información, páginas de encuentro, chats sociales, etc.

Medios con los que se busca reducir costes, incertidumbres y complejidades en la vida de la gente. Justamente, bajo esta misma directriz y premisa, es donde el papel de la tecnología Blockchain es relevante, en consonancia con la revolución digital, dentro de la pretensión pretendida de implantarla en el sistema económico vigente.

2.2. Características, funciones y limitaciones del dinero fiduciario

El dinero fiduciario es un tipo de dinero establecido por medio de una regulación gubernamental como moneda legal y definido por la RAE como “dinero cuyo valor no viene dado por la existencia de unas reservas que lo respalden, sino por la confianza que inspira en su emisor”. El origen de esta evolución del dinero se encuentra en China, en torno al siglo XI. En el siglo XVII llega a Europa occidental, concretamente a Holanda, por medio de los bancos, los cuales emitían “papel moneda” en representación de la cantidad de metal que era ingresado en ellos.

El dinero que se encuentra en circulación es regulado y controlado por diferentes organismos estatales, generalmente los bancos de los países y entidades supranacionales, como el Banco Central Europeo o el Fondo Monetario Internacional. Además de ser los órganos reguladores y emisores, también son los encargados de transmitir y mantener la confianza necesaria en el uso del dinero como medio de pago o bien de inversión.

El valor que posee se deriva del reconocimiento establecido por una autoridad competente -como las que hemos señalado anteriormente o como un gobierno de un país determinado, o porque así lo acuerdan las partes en cuestión- a diferencia del dinero mercancía, cuyo valor era determinado por la valía del metal en cuestión.

Finalmente, cabe señalar que, gracias al dinero fiduciario es posible la existencia de billetes y monedas con valor monetario y curso legal. Técnicamente, el sistema actual se basa en el dinero fiat, una evolución del propio dinero fiduciario, cuya efectividad se debe a la confianza que tiene el receptor en su utilidad como medio de intercambio futuro. El valor que posee el dinero proviene tiene un carácter imperativo,

ya que se encuentra regulado y establecido de forma legal. A pesar de ello, hay situaciones en las que su imposición se convierte en ineficaz al quebrarse la confianza depositada por sus usuarios, como en el caso de las economías ‘hiperinflacionarias’ de Venezuela en la actualidad, o de Alemania tras la Iª Guerra Mundial.

El mayor control sobre la oferta y emisión, la regulación propia que genera menos riesgo y la no escasez de las monedas, son las principales ventajas, que junto a la agilidad y rapidez que proporciona en las transacciones, se pueden destacar de la vigencia y uso del dinero fiduciario en el mercado.

2.3. Paper de Nakamoto⁶

El 31 de octubre de 2008, ‘Satoshi Nakamoto’, publicaba el *whitepaper*⁷ del Bitcoin: “*Bitcoin: A Peer-to-Peer Electronic Cash System*” / “*Bitcoin: Un Sistema de Dinero Electrónico entre Pares*”. Una versión *Peer-to-Peer* (“por pares”) de dinero virtual, cuyo registro de intercambios no necesita de intermediarios ni terceras partes, posibilitando pagos online sin la presencia de una entidad u organismo central. El citado “paper”, planteaba la implementación de la propuesta teórica planteada por Stuart Haber y W. Scott Stornetta (1991).

Cabe destacar el momento en el que tiene lugar la publicación, produciéndose en pleno inicio de una crisis económica global, donde la caída de la entidad bancaria de *Lehman Brothers* en verano de 2007, fue el detonante de una recesión sin precedentes. Sin embargo, este texto revolucionario no representa fielmente el origen propio de esta realidad virtual, ya que en 1991 puede ubicarse su semilla. Stuart Haber y W. Scott Stornetta en este año, desarrollaron un primer trabajo⁸ sobre una cadena concreta de bloques que se encontraban protegidos por un criptograma. Podemos afirmar que, en

⁶ *Whitepaper* del Bitcoin.

⁷ Manifiesto escrito por los creadores de una criptomoneda, recogiendo en él todos los datos, aspectos y características de la misma.

⁸ “*How to time-stamp a digital document*”/ “*Como hacer una marca de tiempo en un documento digital*” (1991).

rasgos generales⁹, la función principal de esta tecnología de cadena de bloques era implementar un sistema de registro de todas las transacciones de los Bitcoins, aportando un marco fiable, rígido y seguro que impida la falsificación de identidades y la seguridad de las transacciones. Para ello, la firma digital (“serie de datos, generados por un método criptográfico, que garantiza la autenticidad de un mensaje o pedido comercial”)¹⁰ y las funciones Hash (“algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud”)¹¹ son vitales. La protección de las transacciones se desarrolla con elementos criptográficos y con el historial de ellas, guardándose en bloques de datos que se agrupan y guardan. Mediante este agrupamiento de los datos se crea una base registrada de movimientos, identidades y cantidades con copia en cada nodo de la red, y que gracias al sistema criptográfico es invariable e imposible de falsificar.

En conclusión, aunque el Bitcoin no ha sido el único proyecto de moneda digital, sí ha sido el más popular y conocido hasta el momento. ‘Satoshi Nakamoto’¹² utilizó esos proyectos anteriores para apoyarse en ellos, aunque el diseño de su modelo eliminó, a diferencia de las bases utilizadas para su realización, la presencia de entidades, organismos o terceros en las transacciones señaladas anteriormente.

⁹ Huillet, M. (2019, 31 de octubre). Hoy se cumplen 11 años del día en que Satoshi Nakamoto publicó el White paper del Bitcoin. *CoinTelegraph*. Recuperado de: <https://es.cointelegraph.com/news/11-years-ago-today-satoshi-nakamoto-published-the-bitcoin-white-paper> [18 de abril de 2021].

¹⁰ Real Academia Española y Consejo General del Poder Judicial, Diccionario panhispánico del español jurídico. Madrid: Santillana, 2017.

¹¹ Donohue, B. (2014, 10 de abril). ¿Qué es un Hash y cómo funciona?. *Kaspersky Daily*. Recuperado de: <https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>). De esta forma, al procesar siempre la misma serie de datos, siempre se obtiene el mismo aspecto del hash en cuestión, mientras que en contra de ello, si es modificado cualquier aspecto o detalle -por mínimo que sea- influirá en el hash resultante.

¹² Pseudónimo utilizado por la persona o personas creadoras del “*Bitcoin: A Peer-to-Peer Electronic Cash System*” / “*Bitcoin: Un Sistema de Dinero Electrónico entre Pares*”, cuya identidad 13 años después sigue sin desvelarse. A pesar de haber expuesto públicamente que se trata de un hombre de 37 años y residente en Japón, son muchas las teorías que sobrevuelan sobre este enigma. Algunas de ellas indican que se trata de un genio o un grupo de personas (Dan Kaminsky), otras rechazan que sea una única persona por el excelente desarrollo del sistema (Laszlo Hanyecz), o incluso Stefan Thomas, aborda el tema de la residencia, poniendo en jaque su ubicación japonesa y situando al sujeto o sujetos en cuestión en América del Norte, América Central, el Caribe y América del Sur.

2.4. Distributed Ledger Technology (DLT)

Distributed Ledger Technology (DLT) / “Tecnología contabilidad distribuida” es un sistema consistente en el registro de transacciones de diferentes activos, registrándose para ello en diferentes sitios a la vez en el tiempo. No existe una entidad o registro central encargado del almacenamiento, mantenimiento y administración general de todos los datos. Este rasgo es el principal en la diferencia con los libros de registro comunes o tradicionales. En este sentido, podemos afirmar que se trata de una gran red a nivel informático repartida en diferentes ubicaciones.

La confianza, tanto en los demás integrantes como en los datos que estos registran, resulta básica para el correcto funcionamiento y fiabilidad de la red. Sin embargo, no siempre es así. Pueden darse situaciones en las que los diferentes integrantes no se pongan de acuerdo, o incluso, se hayan producido errores o engaños en el registro de los datos. Es entonces cuando nos encontramos con “*The Byzantine Generals Problem*” / “El problema de los Generales Bizantinos”.

“*The Byzantine Generals Problems*” podemos definirlos como una serie de mentiras emitidas por sujetos validados de la red, que pretenden alterar la integridad y veracidad del sistema en su beneficio propio y a costa del resto de los integrantes de la red. Tienen su origen en un antiguo juego de lógica. A grandes rasgos, cada integrante de la red tiene encomendada la orden de una transacción concreta, siendo el encargado de transmitírsela a todos los demás. De esta manera, si cualquier otro integrante modifica o engaña sobre tal transacción, tendría la condición de verdadera aquella que consiguiera mayoría en el consenso de todos ellos, logrando ser la afirmación aceptada, y por lo tanto, cualesquiera otras órdenes contradictorias con la aceptada por el consenso, quedarían descartadas. En consecuencia, el sujeto ‘traidor’ o malicioso de la red podría ser identificado neutralizado. Su presencia en la tecnología Blockchain se asocia a las acciones de ciertos nodos malintencionados. Uno de los problemas principales que provoca su existencia en la red es el problema del “*doble gasto*” o

“double spending”¹³: un mismo integrante utiliza en diferentes ocasiones las mismas criptomonedas. Por ejemplo, en el caso del BTC, esta actuación tendría cabida en el caso de que un ‘minero’ tuviera en su poder más del 50% de la capacidad computacional de la red. Contra ello, la red del BTC propone un sistema mediante el cual, la dificultad de resolución del algoritmo que determina el nodo que registra el último bloque de transacciones varía en función de la capacidad computacional de cada nodo integrante de la red. Esta dificultad consta de un parámetro dinámico que de manera periódica se va regulando con el objetivo único de conseguir minar un bloque nuevo en un tiempo ideal de 10 minutos. De esta manera, si la agilidad del sistema se encuentra por encima de esos 10 minutos, la dificultad disminuye y por el contrario, aumentaría.

La “Tecnología de contabilidad distribuida” (DLT) y la tecnología Blockchain tienen puntos comunes y distintivos entre ellos^{14 15}. Teóricamente, comparten origen en la concepción de su existencia: se trata de libros de registro de índole digital y de carácter descentralizado. Sin embargo, la tecnología Blockchain es un tipo de *Distributed Ledger Technology* (DLT). Al mencionar DLT, estamos haciendo referencia a una categoría más amplia que la tecnología Blockchain, al ‘género’ que engloba a un modelo de base de datos que es gestionado a la vez por diferentes participantes, estando descentralizada su gestión y control. Además de la tecnología Blockchain, TEMPO o DAG también se catalogan dentro del ‘mundo DLT’. Es por ello, que en virtud de la definición hecha de la DLT parezca que estamos hablando de la tecnología Blockchain, pues esta sigue esta misma idea con ciertas particularidades propias. En base a esta noción digital, la tecnología Blockchain supone una mayor concreción en el objetivo general de la DLT al incluir en ella la figura de la cadena de bloques (rasgo no esencial de las DLT, ya que estas se caracterizan por constar de una base de datos que se

¹³ Oro y Finanzas (2015, 31 de enero). ¿Cómo se ajusta la dificultad de minado en Bitcoin?. *El Diario Digital del Dinero*. Recuperado de: <https://www.oroymasfinanzas.com/2015/01/como-ajusta-dificultad-minado-bitcoin/> [20 de julio de 2021].

¹⁴ Maldonado, J. (2020, 16 de Julio). DLT vs Blockchain: ¿Cuáles son sus diferencias?. *CoinTelegraph*. Recuperado de: <https://es.cointelegraph.com/explained/dlt-vs-blockchain-what-are-the-differences> [1 de julio de 2021].

¹⁵ Sáez, J. (2021, 1 de julio). ¿Qué son las DLT y en qué se diferencian de Blockchain?. *IEBS*. Recuperado de: <https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/> [1 de julio de 2021].

encuentra distribuida en diferentes lugares a la vez). Tanto los sistemas Blockchain como la tecnología DLT tienen protocolos P2P (*'peer-to-peer'*) que garantizan la seguridad e invariabilidad de los datos contenidos en ellos.

2.5. Funcionamiento de la tecnología Blockchain¹⁶

A la hora de desarrollar la tecnología Blockchain, debemos matizar que no se trata de ninguna aplicación ni de ninguna empresa particular o estatal o global. Podemos definirlo, de forma básica, como un registro de transacciones compartido y verificado por todos los participantes del sistema.

La base de datos de los registros de la Blockchain es compartida. Es decir, cada nodo de la red dispone de una copia común de la base de datos. Los registros incorporados en dicha base se actualizan en función de la información suministrada por cada uno de los participantes (*'nodos'*) de la red Blockchain. Los responsables de los nodos pueden registrar nuevas transacciones en función de los privilegios otorgados por la red, pero no pueden eliminar o *'corregir'* los registros históricos de ésta. De esta manera, los privilegios de registro de nuevas transacciones son verificados (y en su caso validados) por uno o varios de los nodos integrantes de la red. Este proceso de registro y validación garantiza la tolerancia frente a *'fallos bizantinos'* garantizando, de este modo, la seguridad y fiabilidad de la base de datos. Aunque puede parecer compleja en su explicación funcional, la idea es bastante simple. Podemos resumirla de la siguiente forma¹⁷:

- Los participantes reciben el nombre de *'nodo'*, siendo cada uno de ellos un ordenador individual que se conecta a la red (descentralizada o *Peer-to-Peer*). Los nodos son los encargados de guardar la cadena completa que conforma la Blockchain, almacenándose en cada uno de los integrantes de la red una copia idéntica a la de los demás.

¹⁶ Caro, L. (2019). El mercado de las criptomonedas [Trabajo de Fin de Grao en Administración e Dirección de Empresas, 12-15, curso 2018-2019, Facultade de Ciencias Empresariais e Turismo de Ourense, Universidade de Vigo].

¹⁷ *Blockchain: Funcionamiento y utilización*. (2018, 9 de julio). *Central Charts*. Recuperado de: https://www.centralcharts.com/es/gm/1-aprender/1-criptomonedas/42-trading/699-blockchain-funcionamiento-y-utilizacion_ [7 de abril de 2021].

- Cada uno de los participantes emite diferente información (acerca de Bitcoins, alquileres, ventas, etc.), a lo largo de su presencia en la red, a la que se le denomina ‘token’. La información viaja encriptada por la red, lo que hace imposible que se revele el contenido.
- La red se compone de diferentes bloques, recogiendo cada uno de ellos un conjunto de información verificada sobre diferentes transacciones¹⁸. En cada bloque se recoge un código único de identificación con el bloque anterior, un grupo de transacciones recogidas en él y un código único de identificación con el bloque posterior. Esta información, una vez que es realizada la operación en cuestión, se encripta para que sea integrada en la plataforma. Todos ellos son numerados, gracias a su ‘hash’, para poseer un lugar concreto y especificado dentro de la cadena (*recuérdese que Blockchain significa “cadena de bloques”*).
- El proceso de encriptación de la información es realizado por un ‘nodo’. Su labor recae en la comprobación de las transacciones y los ‘hash’¹⁹ correspondientes, verificando la invariabilidad de la transacción. El nodo puede llegar a ser: una persona física -conocida vulgarmente como ‘nodo verificador’ o ‘minero’- o un tercero de confianza del sistema, que suele ser una institución. Es por este último motivo que, existen diferentes tipos de Blockchain, tal y como desarrollaremos posteriormente.
- Todas las transacciones se registran en relación con el momento en el que se producen. Cada una de ellas generan un ‘hash’ propio, que se verá alterado ante cualquier modificación sufrida tanto en ella como en cualquiera de las transacciones con las que se encuentra relacionada. Las transacciones individuales conformarán un ‘bloque’, que será verificado por los nodos ‘verificadores’ o ‘mineros’, para que todas ellas estén relacionadas con la información contenida.

¹⁸ Matizar el término en relación con la tecnología Blockchain, consistiendo en una autorización realizada por un ‘nodo’ en el registro de los Bitcoins asociados a un sujeto emisor y a otro receptor.

¹⁹ Cadena de números y letras creada para distinguir e identificar a cada una de las transacciones realizadas, al igual que para relacionarlas con la transacción anterior y posterior a ella.

- La confianza es clave en el sistema, lo que requiere la presencia de un ‘mecanismo de consenso’²⁰ (Proof of Work, Proof of Stake, Proof of Authority, etc.) entre los diferentes nodos intervinientes. Conviene destacar que, en el caso concreto del Bitcoin, el mecanismo utilizado para lograr el consenso es el ‘Proof of Work’ (‘PoW’): “Proponemos una solución al problema del doble gasto utilizando una red de igual a igual. La red marca la hora de las transacciones al agruparlas en una cadena de prueba de trabajo basada en hash, formando un registro que no se puede cambiar sin rehacer la prueba de trabajo” (Satoshi Nakamoto, 2008).
- El funcionamiento de Proof of Work (‘PoW’) recae en el trabajo requerido a un cliente, que posteriormente es verificado en la red. De esta manera, los diferentes ‘mineros’ entran a competir entre ellos ante un problema criptográfico. El nodo que logra imponerse al resto, es receptor de una recompensa en forma de Bitcoins, junto a las comisiones asociadas a las transacciones en cuestión.
- El proceso se repite infinidad de veces, de tal manera que los nuevos registros que van apareciendo, requieren de una comprobación, verificación y validez otorgada por los nodos de la red.
- Realmente importante es la confianza del sistema, por lo que es vital para su existencia. De esta manera, si hay interés en modificar o actualizar la información de los registros, es necesario el consenso entre la mayoría de los participantes del proceso, mediante el mecanismo Proof of Work (‘PoW’). De especial importancia es que la información introducida nunca podrá ser eliminada.

2.6. Diferentes tipologías en la realidad práctica de la tecnología Blockchain

En su origen, el diseño de esta tecnología pretendía que su uso tuviera un claro carácter público, en donde todos los que así lo quisieran pudieran participar. La

²⁰ “Mecanismo que permite a los usuarios o máquinas coordinarse en un entorno distribuido. Debe garantizar que todos los agentes del sistema puedan ponerse de acuerdo respecto a una fuente única de verdad, incluso en el caso de que algunos de ellos falle”. (*¿Qué es un Algoritmo de Consenso?*. (2018, 13 de diciembre). Academy Binance. Recuperado de: <https://academy.binance.com/es/articles/what-is-a-blockchain-consensus-algorithm#proof-of-work-pow>. [28 de mayo de 2021])

criptomoneda Bitcoin es un ejemplo manifiesto de ello, ya que todo el mundo que lo desee puede participar mediante las transacciones propias. Sin embargo, con el paso del tiempo y la evolución de la tecnología, han aparecido otras formas de Blockchain, no públicas.

2.6.1. Blockchain pública

Es la ‘cadena de bloques’ en la que no existe ningún tipo de restricción respecto a la obtención y verificación de datos y transacciones del proceso. Está caracterizada por una base de datos pública, donde tiene cabida todas las transacciones que se realicen. Cada participante realiza transacciones de manera libre, quedando su registro guardado de manera totalmente transparente.

La comprobación y verificación de esta información es llevada a cabo por los nodos ‘verificadores’ o ‘mineros’. Estos agentes reciben remuneración por cada una de las comprobaciones que realizan. En este aspecto, debemos señalar que el sistema de remuneración depende de la regla de consenso (‘PoW’, ‘PoS’, ‘PoA’) elegida para el sistema en cuestión. No existen figuras intermedias en los procesos, existiendo una total descentralización del proceso. Cualquiera puede unirse a ella. La toma de decisiones en esta tipología se realiza mediante diferentes mecanismos descentralizados y condensados.

- ‘PoW’²¹ (algoritmo de ‘la prueba de trabajo’) es el algoritmo utilizado por el BTC, concebido como un algoritmo de trabajo. Su efectividad reside en que el nodo ‘verificador’ o ‘minero’ verifica la transacción en cuestión tras su proposición, estableciéndose un bloque concreto. De esta manera, se permite a los nodos ‘verificadores’ o ‘mineros’ elegir la cadena de bloques más larga o que ellos pretendan, con el fin de obtener mayor número de incentivos. El alto nivel de potencia informática requerida en su funcionamiento y el aumento en el número de nodos ‘verificadores’ o ‘mineros’ en el último tiempo influyendo en

²¹¿Qué es Proof of Work (PoW)? (s.f.). Academy Bit2me. Recuperado de: <https://academy.bit2me.com/que-es-proof-of-work-pow/>. [17 de mayo de 2021].

la rentabilidad, son los principales impedimentos del algoritmo PoW actualmente.

- ‘PoS’ o algoritmo de ‘la prueba de participación’, es el utilizado por la tecnología Blockchain EOS. ‘PoS’ no concibe en su funcionamiento la presencia de los nodos ‘verificadores’ o ‘mineros’ tan relevantes en la existencia de PoW. Esta característica pretende reducir los costes derivados de la carga computacional soportada por los ‘mineros’. El algoritmo determina los sujetos responsables del bloque en cuestión, otorgando además derechos de voto mediante propiedades aleatorias que impidan la centralización del sistema. Estos sujetos tienen implicación e intereses en los resultados del sistema, y además, responden con el dinero depositado en él, como garantía ante un posible bloqueo provocado deliberadamente.
- ‘PoA’ o algoritmo de ‘la prueba de autoridad’ es el algoritmo utilizado por Oracle Network. Se trata de una red de carácter público con base en ‘Ethereum’, caracterizada por la rapidez y accesibilidad a ella de todos los tipos de miembros, desde multinacionales empresariales a pequeñas y medianas empresas. ‘PoA’ es un procedimiento que genera tasas en menor tiempo que ‘PoW’. En consecuencia, las transacciones y los buques en cuestión son verificados por los ‘validadores’, mediante fases automáticas que requieren de tres requisitos para asegurar su consistencia: verificación producida en la cadena; calificaciones complejas para el logro de incentivos y demostración coherente entre las investigaciones realizadas y los procesos propios.
- Ejemplos de Blockchain pública: Bitcoin, Ethereum, Litecoin (todas ellas basadas en la regla de consenso ‘PoW’).

2.6.2. Blockchain privada

En este caso, nos encontramos con una cadena de bloques en la que la base de datos es totalmente privada. En consecuencia, se trata de un sistema centralizado, en el que una única entidad es la encargada de llevar a cabo el proceso de registro y encriptado. La validación de la invitación a participar a la red recae sobre el creador de la red, o sobre un conjunto de reglas establecidas en la creación. Mediante este tipo de

tecnologías se pretende limitar la participación y realización de transacciones en ella. En estas tecnologías solo se puede participar mediante la invitación y su característica principal es la realización de transacciones en un entorno cerrado, tratando de mejorar la fluidez en la información que poseen los participantes.

- Ejemplos de Blockchain privada: MONAX, Multichain, Blockstack.

2.6.3. Blockchain federales o de consorcio

En último lugar se encuentra un tipo de Blockchain híbrida. En ella, la verificación y el encriptado de los datos es llevado a cabo por uno o unos terceros designados. Por contrario, el modelo de datos es accesible a todos con la limitación de estos terceros, que son los encargados de conceder el acceso a todos aquellos que así lo soliciten. En caso de que no sea aceptado, la accesibilidad quedaba limitada a los participantes de la Blockchain en ese momento.

El consenso es controlado por un grupo de nodos concretos y seleccionados para ello. El derecho a leer la misma puede ser: totalmente público o restringido a los participantes de la red. Su principal utilidad suele ser en el sector bancario y energético.

- Ejemplos de Blockchain federales o de consenso: B3i, R3, EWF.

2.6.4. Síntesis comparativa entre los tres tipos generales de tecnología

Blockchain²²

Tabla 2.1. Elaboración en base a las características recogidas en *Grupo Garatu It Solutions*

TIPOS BLOCKCHAIN	ACCESO	PARTICIPANTES	SEGURIDAD	VELOCIDAD DE TRANSACCIÓN
BLOCKCHAIN PÚBLICAS	Cualquier persona	- Sin permiso - Anónima	Mecanismos de consenso descentralizados	Lenta
BLOCKCHAIN PRIVADAS	Una entidad	- Con permiso - Identidad conocida	Algoritmos de consenso propios (verificación centralizada)	Ágil y rápida

²² ¿Qué tipos de Blockchain o cadenas de bloques existen?. (2018, 8 de noviembre). Grupo Garatu It Solutions. Recuperado de: <https://grupogaratu.com/cuales-son-los-diferentes-tipos-de-blockchains-o-cadena-de-bloques/> [14 de junio de 2021].

TIPOS BLOCKCHAIN	ACCESO	PARTICIPANTES	SEGURIDAD	VELOCIDAD DE TRANSACCIÓN
BLOCKCHAIN FEDERALES O DE CONSORCIO	Organizaciones múltiples seleccionadas	- Con permiso - Identidad conocida	Algoritmos de consenso propios (verificación parcialmente descentralizada)	Ágil y rápida

3. CRIPTOACTIVOS / CRIPTOMONEDAS / CRIPTODIVISAS

3.1. ¿Qué son las criptomonedas? Orígenes y nociones fundamentales

Las criptomonedas, o también denominadas criptoactivos y/o criptodivisas, son monedas digitales creadas y desarrolladas mediante algoritmos, cuyo origen se ubica en *“Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer (2008)”*²³. Estos algoritmos están fundados en la criptografía (“Arte de escribir con clave secreta o de un modo enigmático”)²⁴, utilizando una red (tecnología Blockchain) que garantiza su seguridad. Estas representaciones de valor no son emitidas ni respaldadas por ningún agente público o privado.

La reducción de costes y de tiempo, junto con la limitada presencia e intervención de los poderes y la no presencia de bancos centrales, son otras de las características esenciales de las criptodivisas. Hemos de matizar la existencia de criptomonedas estatales. Se tratan de criptomonedas emitidas por los gobiernos de diferentes países que, siendo similares al Bitcoin, son creadas, puestas en el mercado y avaladas por diferentes estados soberanos, tales como ‘*Yuan Digital*’ (China) o ‘*Petro*’ (Venezuela).

En último lugar, cabe señalar que a pesar de que el comienzo se produjera en 2008, la “gran avalancha” de creaciones de monedas digitales no tuvo lugar hasta tiempo después (‘*Litecoin*’ en 2011, ‘*Dogecoin*’ en 2013, ‘*Ethereum*’ en 2015). A

²³ Nakamoto, S. (2008, 31 de octubre). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin*. Recuperado de: <https://bitcoin.org/bitcoin.pdf>.

²⁴ Real Academia Española. (2001). Diccionario de la lengua española (22.ª ed.). Madrid, España: Autor.

mayores, diferentes países se sumaron a estas nuevas corrientes, creando sus propias criptomonedas.

3.2. Las criptomonedas en la actualidad

Economistas referentes, como Bouveret y Haksar (2018)²⁵, exponen comúnmente tres problemas generales que en la actualidad tienen las criptomonedas:

- No existe ningún organismo o entidad que sustente su uso.
- Poca utilidad como reservas de valor²⁶, al caracterizarse por una alta volatilidad en los precios.
- Reducida aceptación para la realización de pagos.

"La característica principal de las criptomonedas es su anonimato. No creo que esto sea algo bueno. La capacidad de los Gobiernos para encontrar lavado de dinero, evasión de impuestos y financiamiento del terrorismo es algo bueno. En este momento, las criptomonedas se utilizan para comprar fentanilo y otras drogas, por lo que es una tecnología rara que ha causado muertes de manera bastante directa. Creo que la ola especulativa en torno a las ICO y las divisas criptográficas es muy arriesgada para los que van en largo."

Gates, B. (2008)²⁷

No obstante, no todas las posiciones actuales son reticentes a esta nueva realidad monetaria. La anterior directora del Fondo Monetario Internacional afirmó en 2017 que "Un buen día los ciudadanos tal vez preferirán las monedas virtuales, puesto que pueden ofrecer el mismo costo y conveniencia que el efectivo; sin riesgos de liquidación, sin demoras en la compensación, sin registro centralizado, ni intermediarios" (Lagarde, 2017). Por su parte Mike Novogratz, fundador de Galaxy Digital Holdings, remarcaba en 2020: "El Bitcoin va a ser oro digital. Cada vez más personas lo querrán como para

²⁵ Bouveret, A.; Haksar, V. (2018). ¿Qué son las criptomonedas?: la posibilidad de un nuevo tipo de dinero ofrece beneficios y comporta riesgos. *Finanzas y desarrollo: publicación trimestral del Fondo Monetario Internacional y Banco Mundial*, 26-27. Recuperado de: <https://www.imf.org/external/pubs/ft/fandd/spa/2018/06/pdf/basics.pdf>

²⁶ El término hace referencia a aquellos activos que es capaz de mantener su valor sin depreciarse -o hacerlo muy lentamente- haciendo posible la transferencia a un momento concreto futuro del poder adquisitivo presente.

de su cartera”. todo el sistema financiero va a cambiar”²⁷. Además, en contra de la alta volatilidad del Bitcoin hasta la fecha, defiende que en un futuro cercano estabilizará su valor entre los \$3000 y \$6000²⁸. “El Bitcoin a menudo es ridiculizado por ser altamente volátil, pero como oro digital podría desempeñar un papel en una cartera de activos múltiples” (Blokland, 2021)²⁹.

En resumen, se pone de manifiesto que, a pesar de que es una realidad como otra cualquiera con diversas ventajas e inconvenientes, parece existir un debate constante sobre su aplicación, validez e importancia real.

3.3. Tipos de criptoactivos. Principales referentes en el mercado

En la actualidad, podemos encontrarnos con más de 8.400 criptomonedas en circulación en todo el mundo. Nosotros vamos a centrarnos, de forma sintetizada, en el análisis de cinco de las más relevantes³⁰.

3.3.1. Bitcoin (BTC)³¹

Primera y original referencia en el mundo de los activos virtuales, es conocida en el argot como ‘la moneda madre’. Mencionado y desarrollado a lo largo del mismo, su creación se remonta a 2008 en el proyecto “*Bitcoin: A Peer-to-Peer Electronic Cash System*” / “*Bitcoin: Un Sistema de Dinero Electrónico entre Pares*”.

Entre sus particularidades y datos más relevantes, cabe destacar lo expuesto a continuación:

²⁷ Nagarajan, S. (2020, 9 de noviembre). Bitcoin es como el oro digital y no se usará de la misma manera que una moneda tradicional en al menos 5 años, según el inversionista multimillonario Mike Novogratz. *Business Insider México*. Recuperado de: <https://businessinsider.mx/bitcoin-oro-digital-mike-novogratz-criptomonedas/> [1 de junio de 2021].

²⁸ Matos, M. (2019, 8 de enero). ¿Qué fue de la burbuja de las criptomonedas?. *CincoDías*. Recuperado de: https://cincodias.elpais.com/cincodias/2019/01/04/mercados/1546617863_093905.html [15 de abril de 2021].

²⁹ *Bitcoin como oro digital: una perspectiva de múltiples activos*. (2021, 12 de abril). IB. Recuperado de: https://www.infobolsa.es/news/detail?key=20210412472183&source=EI_ULTIMAS [1 de julio de 2021].

³⁰ La referencia a la relevancia de las criptomonedas se realiza teniendo en cuenta el volumen de capitalización ([Página de datos, gráficos y estadísticas de diferentes criptomonedas existentes]. (2021, 4 de junio). *CoinMarketCap*. Recuperado de: <https://coinmarketcap.com/es/currencies>. [4 de junio de 2021]).

³¹ Pacheco, M.N. (2016). Criptodivisas: del Bitcoin al MUFG. El potencial de la tecnología Blockchain. *Revista CESCO de Derecho de Consumo*, 19, 6-15. Recuperado de: <https://revista.uclm.es/index.php/cesco/article/view/1180/952>

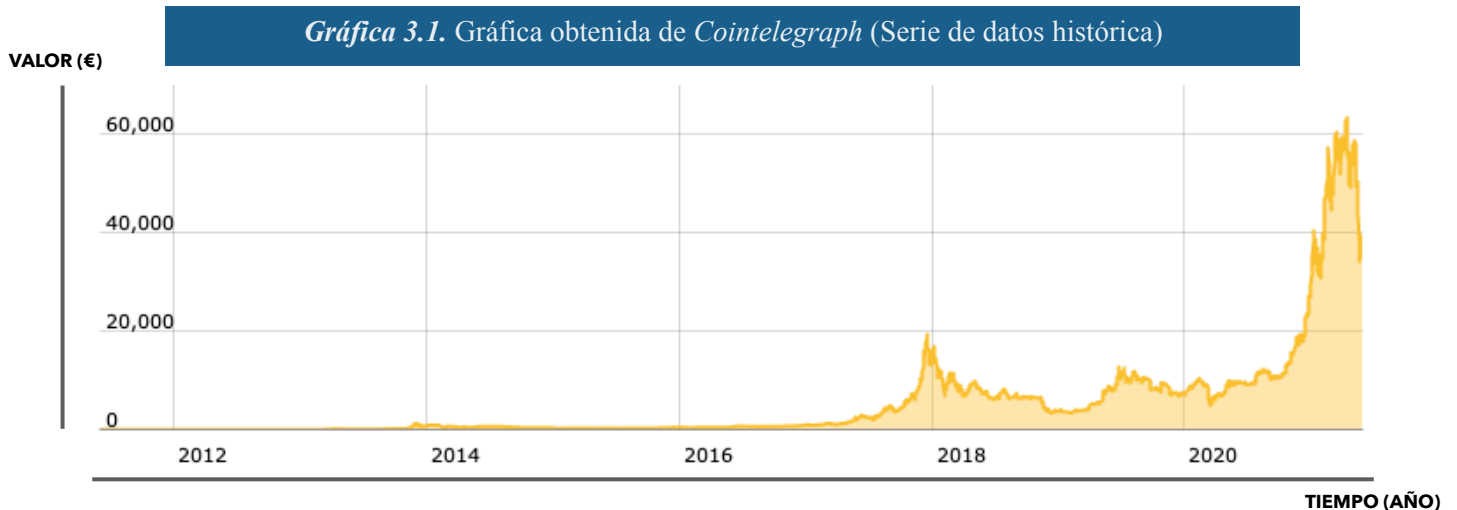
- Se trata de una criptomoneda a 21.000.000 de unidades máximas en circulación, existiendo alrededor de 12.500.000 en la actualidad. Este carácter finito influye en la determinación del valor de BTC y su propósito como activo deflacionario.
- Proof of Work ('PoW') es el algoritmo de consenso propio del Bitcoin. Su funcionamiento consiste en que los nodos 'verificadores' o 'mineros' someten al análisis hash todos los datos que quieren incorporar hasta que logran una solución única y determinada. Se trata de un proceso que proporciona gran seguridad, en el caso de que en la red en cuestión intervenga un elevado número de 'mineros' (a mayor número de 'mineros', mayor seguridad).
- El resto de las criptomonedas se generan mediante un proceso descentralizado denominado 'minado'. Para ello, se recurre al uso de complejos algoritmos y computadoras que resuelven un problema matemático de dificultad variable. El nivel de dificultad está directamente determinado por la capacidad computacional de todos los nodos 'verificadores' o 'mineros' de la red.
- El proceso de 'minado' ("proceso de invertir capacidad computacional para procesar transacciones, garantizar la seguridad de la red y conseguir que todos los participantes estén sincronizados")³² de criptomonedas conlleva recompensas para los 'mineros'. "En el año 2009, los minadores fueron recompensados por 50 BTCs/bloque. Pero según un mandato de Satoshi Nakamoto, las recompensas por minar se reducen a la mitad cada 4 años, reduciéndose a 25 BTCs/bloque en 2012 y a 12,5 BTCs/bloque en 2016. A partir de febrero de este mismo año, los 'mineros' han pasado a ganar 6,25 BTCs por cada bloque minado (equivalente a 330.475 dólares aprox.) Además, se les permite quedarse con las tasas de transacción de cada operación realizada en el bloque, lo que equivale a 20 dólares por cada una de ellas"³³.
- El valor del Bitcoin depende fundamentalmente de su oferta y demanda, aspecto que influye en su predicción y lo hace más complejo.

³² [Página web de preguntas frecuentes]. (2021, 16 de junio). *Bitcoin*. Recuperado de: <https://bitcoin.org/es/faq#que-significa-sincronizando-y-por-que-tarda-tanto>.

³³ *Los mineros de Bitcoin ganaron más de 1.000 millones de dólares el mes pasado: ¿cómo lo lograron?*. (21 de febrero de 2021). iProUP. Recuperado de: <https://www.iproup.com/economia-digital/20746-mineros-de-bitcoin-ganan-fortunas-cuanto-y-de-que-manera>.

- En el momento de su creación, su precio era casi nulo, cuyo registro se sitúa en \$0.03/1BTC aproximadamente. Durante el año 2010, el precio más alto registrado por BTC fue de \$0,39.
- El valor máximo / “All Time High” (ATH) de BTC tiene su registro el 13 de abril de 2021: \$63.106,05 / 1BTC.

3.3.1.1. Evolución histórica del precio de BTC



3.3.2. Ethereum (ETH)

Criptodivisa creada en el año 2013 por el programador ruso Vitalik Buterin. Al igual que BTC, tiene de base una red descentralizada, sistema de *peer-to-peer*, y basado en un sistema tecnológico de cadena de bloques.

Entre sus particularidades y datos más relevantes, cabe destacar lo expuesto a continuación:

- ‘Solidity’ es su propio lenguaje de programación. Éste le permite una implementación mucho más sencilla, facilitándole la posibilidad de llevar a cabo contratos inteligentes y DAPPs (“Término que engloba a aquellas aplicaciones descentralizadas que en su funcionamiento utilizan ‘Blockchain’, facilitando el contacto y la negociación entre los usuarios sin la presencia de un organismo o entidad central que los gestione)³⁴ con más seguridad.

³⁴¿Qué son las DApps y por qué serán cada vez más importantes?. (2019, 22 de febrero). BBVA. Recuperado de: <https://www.bbva.com/es/que-son-las-dapps-y-porque-seran-cada-vez-mas-importantes/>. [16 de junio de 2021]

- ‘Ether’ (ETH) es su criptoactivo propio. Se trata de la segunda moneda digital en términos cuantitativos en volumen de capitalización. Sin embargo, podemos afirmar que Ether es más que una simple criptomoneda, al ser utilizada para la realización de transacciones NFT (“‘Non-Fungible Token’/ ‘Tokens no fungibles’ son representaciones o autorías de posesión de un activo único. Tienen la propiedad de no ser intercambiables entre sí, siendo solo posible su intercambio entre una cantidad determinada de criptomonedas. Además, aportan una prueba de autenticidad y propiedad de un activo en concreto, dentro del sistema inmutable de una Blockchain”)³⁵.
- El valor máximo / “All Time High” (ATH) de ETH tiene su registro el 12 de mayo de 2021: \$4.372 / 1ETH.
- Fue la criptomoneda más negociada en febrero de 2021, con una cifra superior a las 1.300 millones diarias (Bitcoin por su parte, se situó en 283.000/ día).

3.3.2.1. Evolución histórica del precio de ETH

Gráfica 3.2. Gráfica obtenida de *Cointelegraph* (Serie de datos histórica)



3.3.3. Tether (USDT)

Criptomoneda cuya salida al mercado es más reciente, en julio de 2017. Fue creada por Tether Limited y su razón de creación es su vinculación en su valor al dólar. De tal vinculación procede su denominación, siendo esta la abreviación del término ‘USD Tether’.

³⁵ Solé, R. (2021, 19 de junio). Qué son los NFT y para qué sirven. *Profesional Review*. Recuperado de: <https://www.profesionalreview.com/2021/06/19/que-son-nft/>. [27 de mayo de 2021]

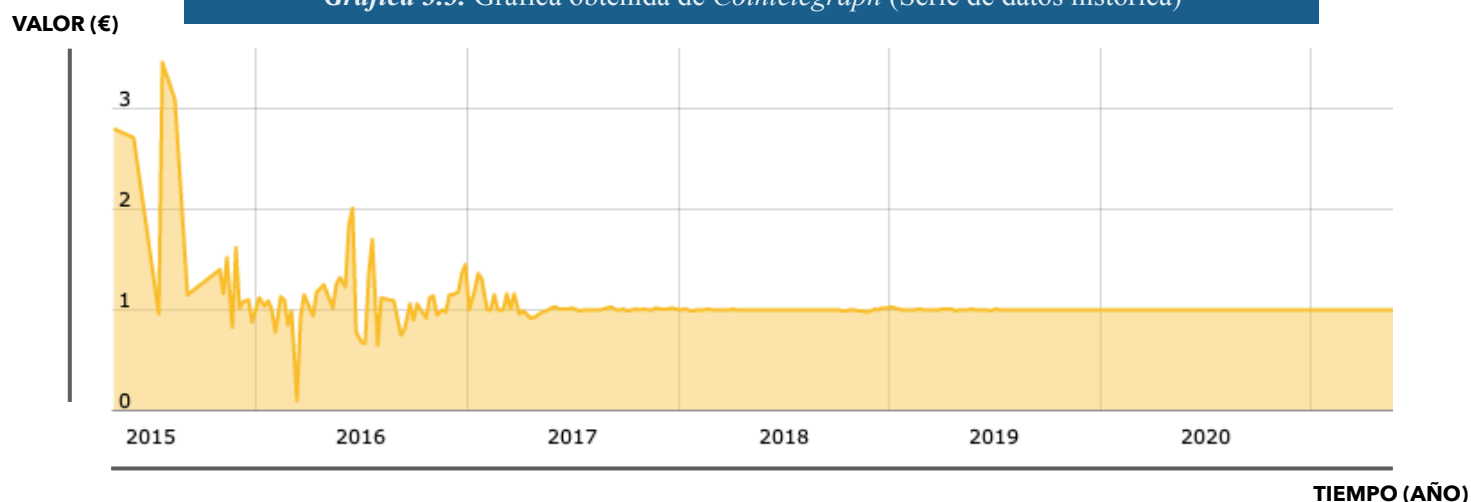
Entre sus particularidades y datos más relevantes, cabe destacar lo expuesto a continuación³⁶:

- La ‘Tether’ (USDT) se encuentra sostenida por una organización privada. En concreto, está 'emitido', 'asegurado' y 'sostenido' por una organización privada. En realidad, es un sistema que puede considerarse centralizado, en la medida en que la emisión de USDT está presumiblemente 'respaldada' por los dólares que mantiene en su poder esta organización.
- Destaca, entre sus principales características, el alto grado de liquidez frente a la gran volatilidad de la mayoría de criptomonedas existentes y su relación 1x1 con el dólar.
- La estabilidad característica de ‘Tether’ imposibilita su proceso de ‘minado’, siendo exclusivamente el ingreso de dinero a la cuenta de la criptomoneda o la compra por intercambio, los únicos procesos posibles para su obtención.
- En algunas ocasiones se han vertido acusaciones afirmando que el fondo de reserva existente de la empresa que lo avala es menor que lo que ésta afirma. En este sentido, en el año 2017 tales acusaciones provocaron la caída del precio a \$0.92 y en 2018 a \$0.89.
- No existe un límite máximo en su emisión y circulación. El número existente en un momento concreto depende directamente de la cantidad de dólares norteamericanos que sirven como contrapartida para este criptoactivo.
- El valor máximo / “All Time High” (ATH) de USDT tiene su registro el 20 de julio de 2015: \$3,46 / 1USDT.

³⁶ ¿Qué es USDT(Tether)?.(s.f.). Academy Bit2me. Recuperado de: <https://academy.bit2me.com/que-es-usdt-theter-criptomoneda/> [11 de junio de 2021]

3.3.3.1. Evolución histórica del precio de USDT

Gráfica 3.3. Gráfica obtenida de *Cointelegraph* (Serie de datos histórica)



3.3.4. Binance Coin (BNB)³⁷

El origen de ‘Binance Coin’ (BNB) se remonta al período comprendido entre el 26 de junio y el 3 de julio del año 2017. Nació mediante un ICO (“El ICO (*‘Initial Coin Offering / ‘Oferta Inicial de Monedas’*) en el campo de las criptomonedas, es el término con el que se hace referencia al proceso, mediante el que se pretende conseguir financiación para una criptodivisa, por medio de su venta, en una fase inicial de su desarrollo)³⁸, previo a la incorporación de que ‘Exchange Binance’ accediera al trading³⁹.

Entre sus particularidades y datos más relevantes, cabe destacar lo expuesto a continuación:

- En ICO inicial recogió 100.000.000 de BNBs. En cambio, en la actualidad la oferta monetaria existente se ha visto reducida como consecuencia de diversas ‘quemadas’ (“hechos periódicos en los que ‘Binance’ destruye BNBs guardados en su tesorería, eliminando así monedas en circulación y reduciendo la cantidad total. Los eventos de quema de BNB están programados para realizarse cada trimestre hasta que 100,000,000 BNB sean finalmente destruidas, lo que

³⁷ ¿Qué es BNB?. (2018, 28 de noviembre). Academy Binance. Recuperado de: https://academy.binance.com/es/articles/what-is-bnb_ [27 de mayo de 2021]

³⁸ ¿Qué son las ICO de criptomonedas?. (s.f.). Academy Bit2me. Recuperado de: <https://academy.bit2me.com/ico-criptomonedas/>. [17 de mayo de 2021]

³⁹ Proceso financiero en el que tiene lugar la compra y venta de activos cotizados con la característica esencial de su elevada liquidez.

representa el 50% del total de BNB alguna vez emitido (200,000,000 de BNB))⁴⁰. Uno de los principales inconvenientes de BNB reside en la alta concentración que mantienen sus fundadores sobre él (40% del total), haciendo posible que puedan manipularlo.

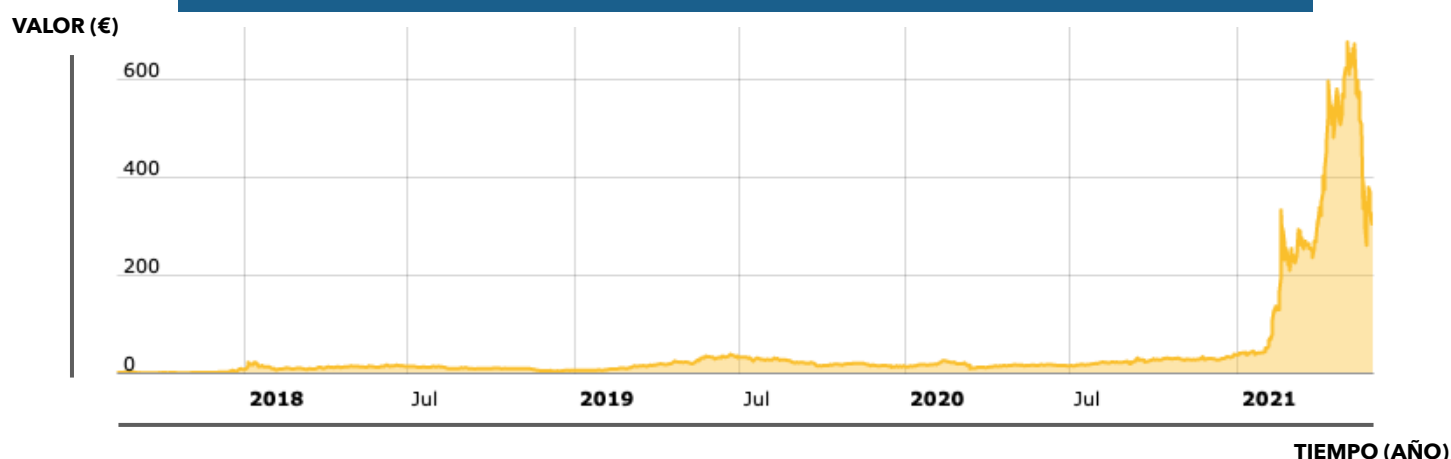
- A diferencia de otras criptomonedas, gracias a BNB es posible la compraventa del resto de criptodivisas dentro de su sistema. Esto hace que las transacciones con BNB sean más baratas.
- El número máximo de BNB en circulación se encuentra estipulado en 200.000.000 unidades.
- Su funcionamiento se caracteriza por la presencia de un “campo Memo” al llevarse a cabo el envío de BNB. De esta manera, por medio de caracteres se pretende identificar y determinar a los sujetos intervinientes en la operación.
- Utiliza un medio de clústeres⁴¹ para garantizar los fondos monetarios.
- Se trata de una criptomoneda con gran aceptación en el mercado, lo que posibilita su uso como medio de pago en diferentes servicios, tanto digitales como comercios físicos (a finales de 2018, BNB era aceptada en más de 150 establecimientos).
- Esta criptomoneda utiliza el protocolo BFT (‘Tolerancia a Fallas Bizantinas’) que permite controlar los problemas por medio de validadores y bloques de verificación.
- El valor máximo / “All Time High” (ATH) de BNB tiene su registro el 12 de abril de 2021: \$610 / 1BNB.

⁴⁰ *¿Qué es una quema de monedas?* (2018, 9 de diciembre). Academy Binance. Recuperado de: <https://academy.binance.com/es/articles/what-is-a-coin-burn>. [10 de julio de 2021]

⁴¹ Conjunto de servidores que operan en conjunto en la red, de modo que el resultado es mayor que si lo hiciera uno solo pero al mismo tiempo trabajan de modo unitario.

3.3.4.1. Evolución histórica del precio de BNB

Gráfica 3.4. Gráfica obtenida de *Cointelegraph* (Serie de datos histórica)



3.3.5. Cardano (ADA)

En 2015 comenzó el desarrollo de esta quinta criptomoneda que estudiamos, a siendo lanzada finalmente en el año 2017. IOHK fue la empresa protagonista del lanzamiento es la empresa que llevó a cabo dicho lanzamiento, junto con la Fundación Cardano y Emurgo. Su nombre se debe a Girolamo Cardano y su criptomoneda, ADA, en referencia a Ada Lovelace.

Entre sus particularidades y datos más relevantes, cabe destacar lo expuesto a continuación⁴²:

- ADA es la cuarta criptomoneda más importante en términos de capitalización.
- Su proyecto y realidad ha sido ‘blanco’ de muchas críticas, al ser considerado por muchos sectores como “un proyecto poco original e híbrido entre los propios de BTC y ETH”.
- ‘Cardano’ es la plataforma sobre la que recae el funcionamiento, siendo diseñada por un equipo de ingenieros, que desde su origen pretendieron conseguir el primer proyecto de tecnología Blockchain con bases en la filosofía científica. Su objetivo prioritario era la implementación de un proyecto pionero en tecnología Blockchain con arraigo en la filosofía científica.

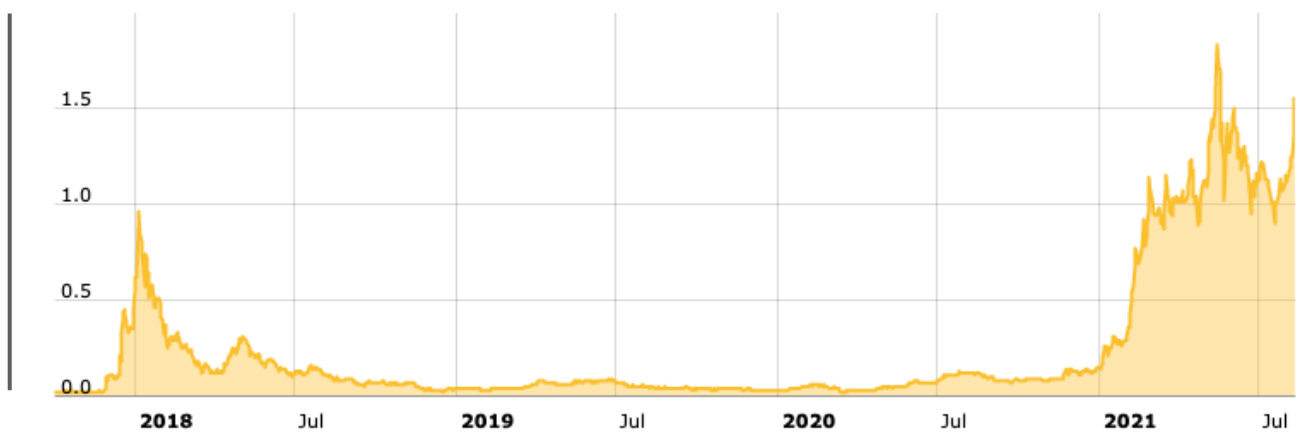
⁴² Quirós, F. (2020, 16 de julio). ¿Qué hace que Cardano tenga características diferentes a otras plataformas Blockchain?. *CoinTelegraph*. Recuperado de: <https://es.cointelegraph.com/news/what-makes-cardano-different-from-other-blockchain-platforms> [12 de mayo de 2021].

- En su funcionamiento utiliza 'Ouroboros', un algoritmo Proof of Stake (“Es un algoritmo de consenso que recompensa las ganancias en función al número de monedas que se poseen. Cuanto más inviertas en la moneda más ganarás con este protocolo”)⁴³ para determinar el consenso de la red. Sintetizando su estructura, se divide en dos grupos o capas. La primera de ellas, CSL, es la encargada de llevar a cabo la función de libro contable que requiere a la presencia de ‘PoS’ para producir bloques y validar las diferentes transacciones. CCL es la segunda, y engloba en ella la información relativa a todas las transacciones que han tenido lugar. La ventaja principal de esta doble categorización en dos fases es la creación de diferentes reglas en la evaluación de las transacciones realizada.
- ADA es el token propio de Cardano, situada entre las 10 criptomonedas más importantes y teniendo un volumen de capitalización superior a los 8.000.000 €.
- El valor máximo / “All Time High” (ATH) tiene su registro el 15 de mayo de 2021: \$1,830 / 1ADA.

3.3.5.1. Evolución histórica del precio de ADA

Gráfica 3.5. Gráfica obtenida de Cointelegraph (Serie de datos histórica)

VALOR (€)



TIEMPO (AÑO)

⁴³ [Blog con contenido de glosario Blockchain, términos y definiciones]. (2021, 8 de julio). *Bitcobie*. Recuperado de: <https://www.bitcobie.com/glosario-blockchain/>.

4. ANÁLISIS COMPARATIVO DE REFERENCIAS DEL MERCADO DE CRIPTOACTIVOS

4.1. Principales valores de las criptomonedas estudiadas: BTC, ETH, USDT, BNB y ADA

Tabla 4.1. Tabla de elaboración propia en base a los datos obtenidos de *Cointelegraph*

VALOR/ REFERENCIA	BTC	ETH	USDT	BNB	ADA
PRECIO (28/06/2021)	\$36.510,96	\$2.530,16	\$1	\$332,22	\$1,54
VOLUMEN DE COMERCIO ÚLTIMAS 24H.	\$49.966 mills.	\$36.229 mills.	\$107.719 mills.	\$4.195 mills.	\$4.990 mills.
DOMINIO DE MERCADO	42,82 %	18,63 %	3,82 %	3,22 %	3,07 %
CAPITALIZACIÓN DE MERCADO	\$686.817 mills.	\$299.358 mills.	\$51.579 mills.	\$49.044 mills.	\$61.210 mills.
VARIACIÓN (ÚLTIMO DÍA) * A día de 28 de mayo de 2021	-2,14 %	-5,27 %	-0,08 %	-3,17 %	-7,59 %
MÁXIMO (TODOS LOS TIEMPOS)	\$64.863,1	\$4.362,35	\$690,93	\$2,46	\$1,21
MÍNIMO (TODOS LOS TIEMPOS)	\$65,53	\$0,4209	\$0,8995	\$0,09611	\$0,01735
ROI*	27.088,02 %	90.942,26 %	0,14 %	291.707,4 %	6.981,51 %
Nº TOTAL TOKENS EN CIRCULACIÓN	18,7 mills.	116,059 mills.	61.125,9 mills.	153,4 mills.	31.948,3 mills.
% DE TOKENS EN CIRCULACIÓN SOBRE TOKENS TOTALES	100 %	100 %	90,56 %	70,99 %	97,84 %

4.2. Variación porcentual en el precio de las criptomonedas estudiadas (BTC, ETH, USDT, BNB, ADA) con respecto a la relativa a los índices bursátiles S&P 500 e IBEX 35 en los últimos 5 años

Tabla 4.2. Tabla de elaboración propia en base a los datos obtenidos de *Investing*

PERÍODO TEMPORAL	1/01/2017 - 1/01/2018	1/01/2018 - 1/01/2019	1/01/2019 - 1/01/2020	1/01/2020 - 1/01/2021	1/01/2021 - 04/06/2021
BTC	965,60 %	-75,20 %	152,00 %	360,10 %	386,70 %
ETH	13.876,06 %	-85,52 %	36,40 %	915,98 %	208,97 %
USDT	5,5207 %	-2,4602 %	0,0315 %	-0,3872 %	-0,0223 %
BNB	324,62 % ⁴⁴	-27,08 %	198,14 %	222,46 %	712,22 %
ADA	19,02 % ⁴⁵	-94,62 %	32,85 %	951,03 %	662,92 %
S&P 500	26,13 %	1,14 %	28,67 %	14,96 %	14,41 %
IBEX 35	11,76 %	-9,83 %	9,70 %	-18,76 %	9,26 %

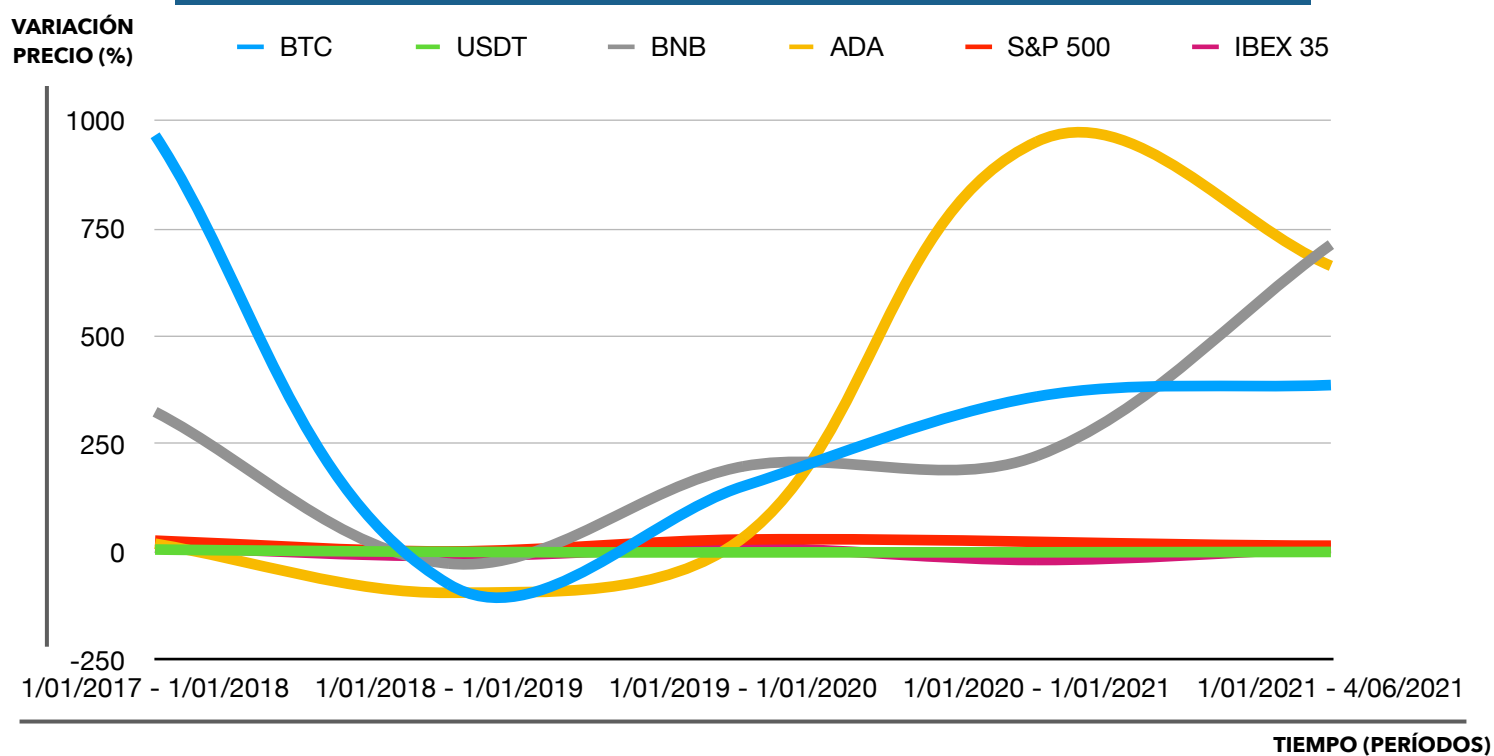
4.2.1. Exposición gráfica conjunta de las variaciones recogidas en apartado 4.2.

*Debido al alto valor de la variación de ETH, del período temporal de 1/01/2017-1/01/2019, en proporción con el resto de valores recogidos en la tabla, se recoge en la gráfica 3.8 el conjunto de las variaciones del resto de criptomonedas e índices protagonistas de la tabla 3.7., a excepción de ETH, cuya variación porcentual en el precio se expone gráficamente a continuación de manera individual (Gráfica 3.9. - p.40).

⁴⁴ Se tiene en cuenta el día 9/11/2017 al ser el primero en el que se tiene registro de BNB.

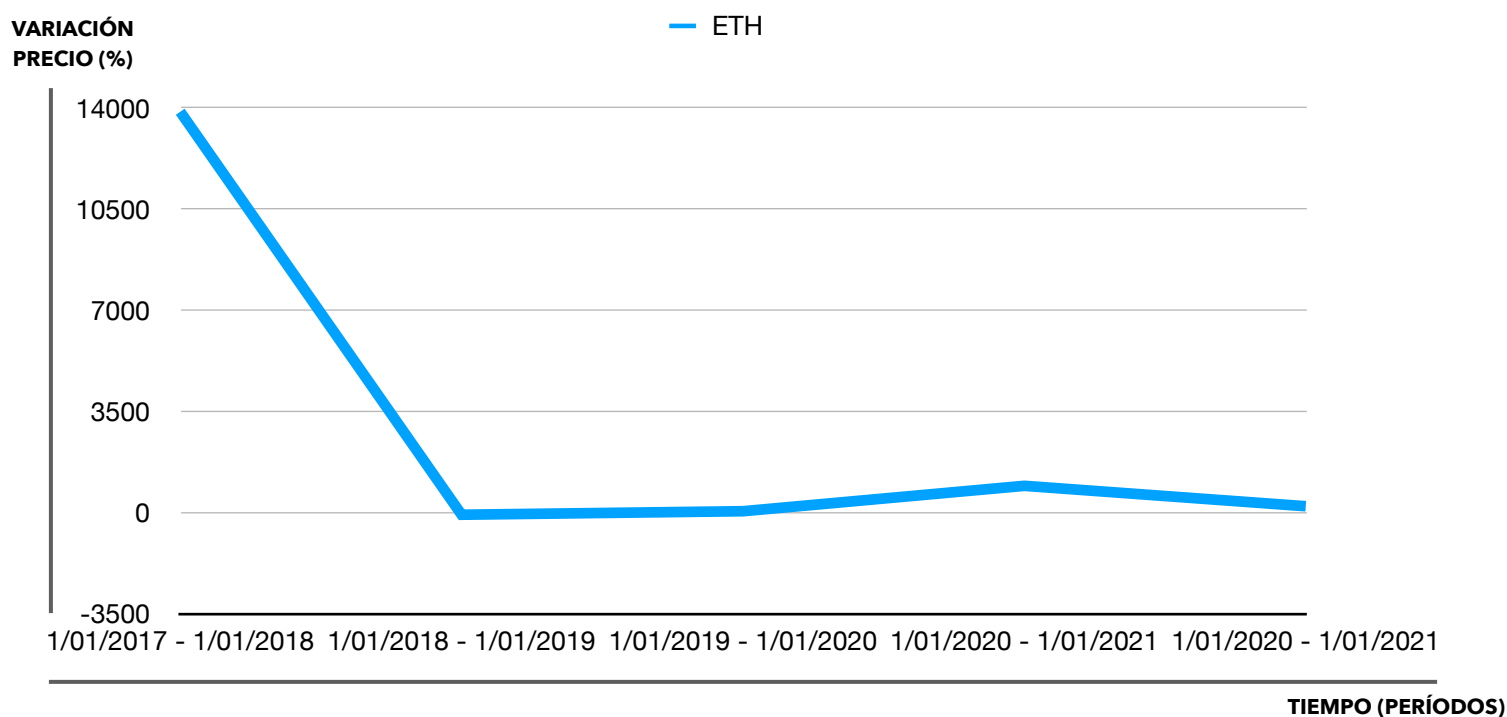
⁴⁵ Se tiene en cuenta el día 31/12/2017 al ser el primero en el que se tiene registro de ADA.

Gráfica 4.3. Gráfica realizada en base a los datos de la tabla 4.2.



i

Gráfica 4.4. Gráfica realizada en base a los datos de la tabla 4.2.



4.3. Ranking global de las 10 critpomonedas con mayor valor en el mercado actual⁴⁶⁴⁷

Tabla 4.5. Tabla de elaboración propia en base a los datos obtenidos de *Statista Global Consumer Survey*

CRIPTOMONEDA	VALOR EN DÓLARES
Yearn.finance (YFI)	\$52.211,36
Wrapped Bitcoin (WBTC)	\$40.111,65
Bitcoin BEP2 (BTCB)	\$39.804,08
Bitcoin	\$39.797,01
Maker (MKR)	\$3.734,75
Ethereum (ETH)	\$2.712,07
Bitcoin Cash (BCH)	\$798,73
Compound (COMP)	\$518,48
Aave (AAVE)	\$458,61
Kusama (KSM)	\$420,25

4.4. Ranking global de las 10 criptomonedas con mayor volumen de negociación en el mercado actual⁴⁸⁴⁹

Tabla 4.6. Tabla de elaboración propia en base a los datos obtenidos de *Statista Global Consumer Survey*

CRIPTOMONEDA	VOLUMEN DE NEGOCIACIÓN EN DÓLARES
Tether (USDT)	\$153,65 mills.
Bitcoin (BTC)	\$70,45 mills.
Ethereum (ETH)	\$31,56 mills.
Ripple (XRP)	\$30,78 mills.

⁴⁶ Fernández, R. (2021, 17 de junio). Criptodivisas más valiosas a nivel mundial en mayo de 2021. *Statista Global Consumer Survey*. Recuperado de: <https://es.statista.com/estadisticas/657235/monedas-virtuales-mas-valoradas-a-nivel-mundial/>. [25 de mayo de 2021].

⁴⁷ Los datos reflejados en la tabla 3.10. tienen su validez a fecha de 20 de mayo de 2021.

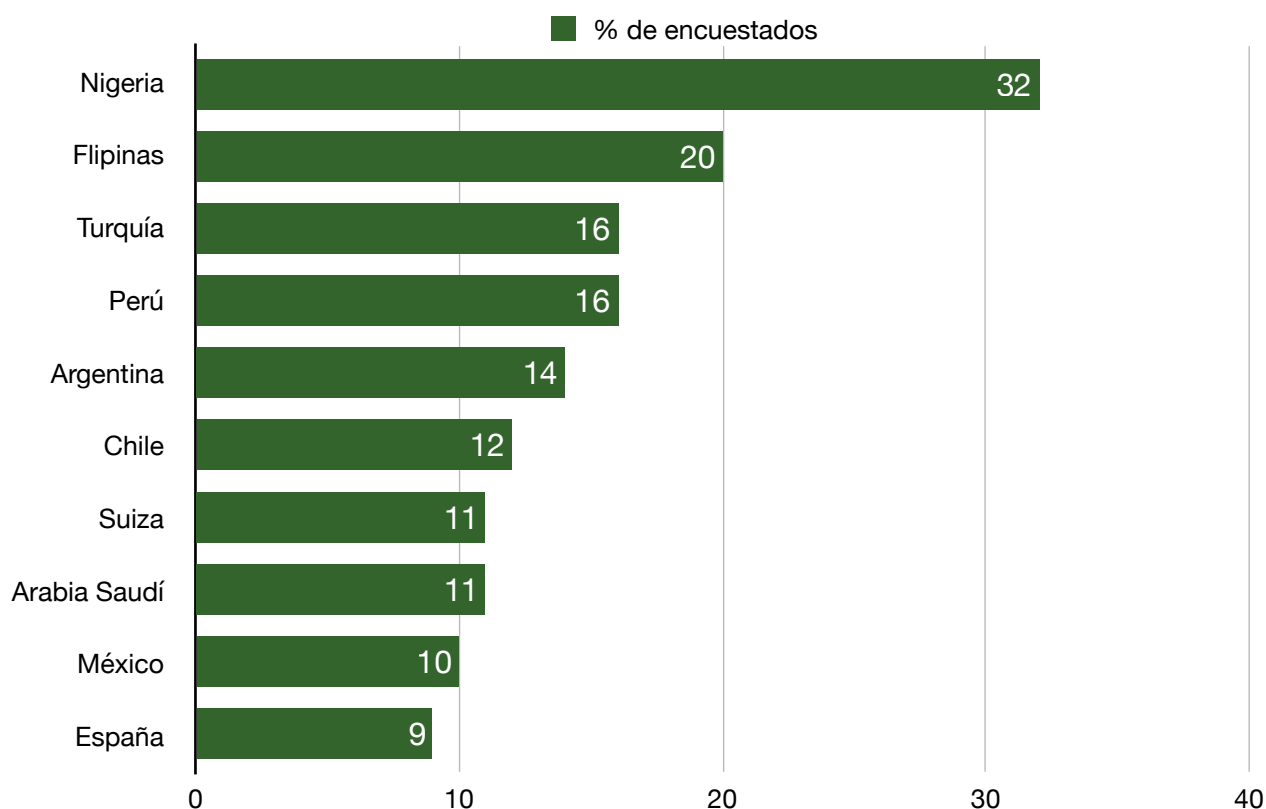
⁴⁸ Fernández, R. (2021, 14 de mayo). Principales criptomonedas por volumen de negociación a nivel mundial mayo 2021. *Statista Global Consumer Survey*. Recuperado de: <https://es.statista.com/estadisticas/657259/principales-criptomonedas-por-volumen-de-negociacion-a-nivel-mundial/>. [26 de mayo de 2021].

⁴⁹ Los datos recogidos en la tabla 3.11. tienen su validez a fecha de 14 de mayo de 2021.

CRIPATOMONEDA	VOLUMEN DE NEGOCIACIÓN EN DÓLARES
Dogecoin (DOGE)	\$17,50 mills.
Tron (TRX)	\$9,19 mills.
Cardano (ADA)	\$8,20 mills.
Binance Coin (BNB)	\$8,11 mills.
Binance USD (BUSD)	\$7,45 mills.
Litecoin (LTC)	\$7,30 mills.

4.5. Clasificación de los 10 países a nivel mundial con mayor demanda de sus ciudadanos en el mercado de las criptomonedas⁵⁰⁵¹

Gráfica 4.7. Gráfica de elaboración propia en base a los datos obtenidos en Statista Global Consumer Survey



⁵⁰ Mena, M. (2021, 23 de marzo). La adopción de las criptomonedas en el mundo. *Statista Global Consumer Survey*. Recuperado de: <https://es.statista.com/grafico/18425/adopcion-de-las-criptomonedas-en-el-mundo/>. [3 de julio de 2021].

⁵¹ Los porcentajes reflejados en la gráfica 3.12. son los resultados de una encuesta online realizada por *Statista Global Consumer Survey* desde febrero a noviembre de 2020, con muestras de 2.000 a 25.000 personas, en cada uno de los 74 países seleccionados. El concepto de la misma es “¿Qué tan comunes son las criptomonedas en el mundo?”, recogiendo el porcentaje de aquellos encuestados que “afirman usar o poseer criptomonedas”.

5. CONCLUSIONES

- I. La evolución del dinero -en los diferentes formatos y en aplicación de los diversos sistemas que han existido a lo largo de la historia- es el resultado del propio desarrollo del hombre y la sociedad. El futuro, y en gran parte ya el presente, está marcado por la presencia del dinero digital que desde 2009 ha revolucionado el mundo monetario.
- II. Los ‘criptoactivos (‘criptomonedas’ o ‘criptodivisas’) no son únicamente validos como medios de pago, sino que además tienen un papel relevante en el campo de las inversiones financieras. La rapidez de sus transacciones potencia su utilidad como instrumentos de inversión, agilizando y simplificando el modelo habitual.
- III. La importancia del Bitcoin, por su condición de criptomoneda pionera, no es mayor que la de la tecnología Blockchain. El desarrollo del presente trabajo me ha servido para apreciar tal relevancia. Para el ciudadano medio mundial -teniendo como referencia mi propio conocimiento previo al desarrollo del trabajo- la trascendencia de la tecnología Blockchain puede pasar desapercibida por el protagonismo del Bitcoin. Sin embargo, el soporte tecnológico de la plataforma Blockchain es fundamental, ya que es el medio en el que se realizan todas las transacciones de las criptomonedas, bajo sus insignias de la seguridad y el anonimato. Además, la red de carácter ‘P2P’ (*peer-to-peer*) posibilita un marco práctico sin intermediarios y descentralizado.
- IV. Personalmente, y a diferencia de mi noción inicial en el momento de comenzar con el desarrollo del trabajo, la seguridad que presenta el sistema ha sido uno de los valores que mayor atención me ha suscitado durante el estudio. La presencia de la criptografía en todos los modelos de la tecnología Blockchain y en su aplicación en las diferentes criptomonedas, proporciona un alto nivel de seguridad e integridad en las transacciones y en la información. Se trata de un rasgo de gran valor por el alto nivel de amenazas que nos encontramos a día de hoy en Internet, por medio de estafas, robos de contraseñas, falsificaciones de cuentas o manipulaciones de cuentas bancarias, entre otros.

- V. El gran abanico de criptomonedas existentes es otro de los aspectos que en mayor medida me ha suscitado gran impacto. En la actualidad, más de 10.000 criptodivisas coexisten. El ‘desplome’ del Bitcoin desde mayo del año 2021, cuando llegó a bajar a un 35% su valor, y la captación que esta moneda tiene del total del mercado: un 40% aproximadamente (a comienzos de año representaba el 70%), denotan un movimiento de cierta independencia del sistema en relación con el Bitcoin y ‘su hegemonía’; inaugurando una nueva época para el resto de las criptomonedas.
- VI. El auge del mercado de las criptomonedas parece no ser algo efímero, sino más bien, una certeza establecida en el sistema financiero vigente. A pesar de las regulaciones sufridas en China o las afirmaciones de Elon Musk, CEO de *Tesla Motors*: "cuando se confirme un uso razonable (al menos un 50%) de energía limpia por parte de los mineros con una tendencia futura positiva, Tesla volverá a permitir las transacciones de Bitcoin"⁵², entre otros, la realidad global se ha acercado al universo de las criptomonedas. No se trata de afirmación en balde, sino una aserción que se corrobora con los datos señalados en la *gráfica 3.7*. La mayor constatación que extraemos de ella es que, el desarrollo, el nivel social y las posibilidades económicas de los países no influyen en el nivel de presencia de las criptomonedas. Liderando Nigeria con un 32%, y seguido de Filipinas (20%) y Turquía (16%), se manifiesta tal percepción personal.
- VII. La alta volatilidad de la mayoría de las criptomonedas, a excepción de USDT -gran estabilidad y relación 1x1 con el dólar-, con bajas y subidas de valor de gran calado en periodos temporales cortos, se refleja en la comparativa analítica proporcionada en las tablas y gráficas del apartado 4 (*‘Análisis comparativo de diversas referencias del mercado de criptoactivos’*). Sin embargo, los índices bursátiles mantienen una línea regularmente horizontal, con pequeñas variaciones positivas y negativas. Por ende, la inestabilidad de las criptodivisas se contrapone a la regularidad propia de los índices bursátiles, manifestándose tal diferencia esencial entre ambos tipos de inversiones.

⁵² Becedas, M.; Nieves, V. (2021, 17 de junio). El Bitcoin y las criptomonedas se enfrentan a un mercado bajista que aún tiene recorrido. *El Economista*. Recuperado de: <https://www.eleconomista.es/mercados-cotizaciones/noticias/11276979/06/21/El-bitcoin-y-las-criptomonedas-se-enfrentan-a-un-mercado-bajista-que-aun-tiene-recorrido.html> [21 de junio de 2021].

VIII. Analizando en conjunto los datos recogidos no podemos hacer mención, a priori, de ninguna relación directa o indirecta de correlación entre los diferentes criptoactivos estudiados, no pudiendo establecer conexión alguna entre las subidas porcentuales de uno con las bajadas de otro, o con la firmeza de un tercero. A pesar de ello, en el período 1/01/2017 - 1/01/2019, BTC, ADA, BNB y ETH ‘caen’ porcentualmente -en diferente magnitud-, protagonizando una subida todos ellos cercana en el tiempo. Sin embargo, es justo cuando este crecimiento comienza cuando la tendencia de cada uno de ellos se vuelve dispar. En los períodos sucesivos a 1/01/2019 - 1/01/2020, la propensión en la variación de los precios de las diferentes criptodivisas no presenta ningún tipo de secuencia general entre ellos, creciendo y disminuyendo en desiguales cuantías.

6. BIBLIOGRAFÍA

Becedas, M.; Nieves, V. (2021, 17 de junio). El Bitcoin y las criptomonedas se enfrentan a un mercado bajista que aún tiene recorrido. *El Economista*. Recuperado de: <https://www.eleconomista.es/mercados-cotizaciones/noticias/11276979/06/21/El-bitcoin-y-las-criptomonedas-se-enfrentan-a-un-mercado-bajista-que-aun-tiene-recorrido.html> [21 de junio de 2021]

Bedecarratz, F. (2018). Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal. *Revista chilena de derecho y tecnología*, 1, 79-105. Recuperado de: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000100079. [2 de junio de 2021]

[Blog con contenido de glosario Blockchain, términos y definiciones]. (2021, 8 de julio). *Bitcobie*, Recuperado de: <https://www.bitcobie.com/glosario-blockchain/>.

[Página web de preguntas frecuentes]. (2021, 16 de junio). *Bitcoin*. Recuperado de: <https://bitcoin.org/es/faq#que-significa-sincronizando-y-por-que-tarda-tanto>.

Bitcoin como oro digital: una perspectiva de múltiples activos. (2021, 12 de abril). IB. Recuperado de: https://www.infobolsa.es/news/detail?key=20210412472183&source=EI_ULTIMAS. [1 de julio de 2021]

Blockchain: Funcionamiento y utilización. (2018, 9 de julio). *Central Charts*. Recuperado de: https://www.centralcharts.com/es/gm/1-aprender/1-criptomoneda/42-trading/699-blockchain-funcionamiento-y-utilizacion__ [7 de abril de 2021]

- Bouveret, A.; Haksar, V. (2018). ¿Qué son las criptomonedas?: la posibilidad de un nuevo tipo de dinero ofrece beneficios y comporta riesgos. *Finanzas y desarrollo: publicación trimestral del Fondo Monetario Internacional y Banco Mundial*, 26-27. Recuperado de: <https://www.imf.org/external/pubs/ft/fandd/spa/2018/06/pdf/basics.pdf>
- Caro, L. (2019). El mercado de las criptomonedas [Trabajo de Fin de Grao en Administración e Dirección de Empresas, 12-15, curso 2018-2019, Facultade de Ciencias Empresariais e Turismo de Ourense, Universidade de Vigo].
- [Página de datos, gráficos y estadísticas de diferentes critpomonedas existentes]. (2021, 4 de junio). *CoinMarketCap*. Recuperado de: <https://coinmarketcap.com/es/currencies>. [4 de junio de 2021].
- Dolader, C.; Bel, J.; Muñoz, J.L. (2017). La Blockchain: Fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Revista Economía Industrial*, 405, 33-40. Recuperado de: <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf>
- Donohue, B. (2014, 10 de abril). ¿Qué es un Hash y cómo funciona?. *Kaspersky Daily*. Recuperado de: <https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/> [17 de julio de 2021]
- Fernández, R. (2021, 17 de junio). Criptodivisas más valiosas a nivel mundial en mayo de 2021. *Statista Global Consumer Survey*. Recuperado de: <https://es.statista.com/estadisticas/657235/monedas-virtuales-mas-valoradas-a-nivel-mundial/>. [25 de mayo de 2021]
- Fernández, R. (2021, 14 de mayo). Principales criptomonedas por volumen de negociación a nivel mundial mayo 2021. *Statista Global Consumer Survey*. Recuperado de: <https://es.statista.com/estadisticas/657259/principales-criptomonedas-por-volumen-de-negociacion-a-nivel-mundial/>. [26 de mayo de 2021]
- Fernández, Y. (2018, 19 de mayo). Los argumentos de Bill Gates en contra del Bitcoin e Hyperloop, y a favor de la IA y los coches eléctricos. *Xataka*. Recuperado de: <https://www.xataka.com/criptomonedas/los-argumentos-de-bill-gates-en-contradel-bitcoin-e-hyperloop-y-a-favor-de-la-ia-y-los-coches-electricos>. [23 de abril de 2021]
- Gates, B. (2018, 27 de febrero). “Ask Me Anything” (AMA). *Reddit*. Recuperado de: <https://www.xataka.com/criptomonedas/los-argumentos-de-bill-gates-en-contradel-bitcoin-e-hyperloop-y-a-favor-de-la-ia-y-los-coches-electricos>. [19 de julio de 2021]

- Huillet, M. (2019, 31 de octubre). Hoy se cumplen 11 años del día en que Satoshi Nakamoto publicó el White paper del Bitcoin. *CoinTelegraph*. Recuperado de: <https://es.cointelegraph.com/news/11-years-ago-today-satoshi-nakamoto-published-the-bitcoin-white-paper> [18 de abril de 2021]
- [Página de datos, gráficos y estadísticas de diferentes criptomonedas existentes]. (2021, 4 de junio). *Investing*. Recuperado de: <https://es.investing.com/crypto>.
- Lagarde, C. (2017, 29 de septiembre). Los Bancos centrales y la tecnología financiera: ¿un mundo feliz?. *IMF*. Recuperado de: <https://www.imf.org/es/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>.
- Los mineros de Bitcoin ganaron más de 1.000 millones de dólares el mes pasado: ¿cómo lo lograron?*. (21 de febrero de 2021). iProUP. Recuperado de: <https://www.iproup.com/economia-digital/20746-mineros-de-bitcoin-ganan-fortunas-cuanto-y-de-que-manera>.
- Maldonado, J. (2020, 16 de Julio). DLT vs Blockchain: ¿Cuáles son sus diferencias?. *CoinTelegraph*. Recuperado de: <https://es.cointelegraph.com/explained/dlt-vs-blockchain-what-are-the-differences> [1 de julio de 2021]
- Matos, M. (2019, 8 de enero). ¿Qué fue de la burbuja de las criptomonedas?. *CincoDías*. Recuperado de: https://cincodias.elpais.com/cincodias/2019/01/04/mercados/1546617863_093905.html [15 de abril de 2021]
- Mena, M. (2021, 23 de marzo). La adopción de las criptomonedas en el mundo. *Statista Global Consumer Survey*. Recuperado de: <https://es.statista.com/grafico/18425/adopcion-de-las-criptomonedas-en-el-mundo/>. [3 de julio de 2021]
- Nagarajan, S. (2020, 9 de noviembre). Bitcoin es como el oro digital y no se usará de la misma manera que una moneda tradicional en al menos 5 años, según el inversionista multimillonario Mike Novogratz. *Business Insider México*. Recuperado de: <https://businessinsider.mx/bitcoin-oro-digital-mike-novogratz-criptomonedas/> [1 de junio de 2021]
- Nakamoto, S. (2008, 31 de octubre). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin*. Recuperado de: <https://bitcoin.org/bitcoin.pdf>
- Oro y Finanzas (2015, 31 de enero). ¿Cómo se ajusta la dificultad de minado en Bitcoin?. *El Diario Digital del Dinero*. Recuperado de: <https://www.oroymasfinanzas.com/2015/01/como-ajusta-dificultad-minado-bitcoin/> [20 de julio de 2021]
- Pacheco, M.N. (2016). Criptodivisas: del Bitcoin al MUFG. El potencial de la tecnología Blockchain. *Revista CESCO de Derecho de Consumo*, 19, 6-15. Recuperado de: <https://revista.uclm.es/index.php/cesco/article/view/1180/952>

- ¿Qué es BNB?. (2018, 28 de noviembre). Academy Binance. Recuperado de: https://academy.binance.com/es/articles/what-is-bnb_ [27 de mayo de 2021]
- ¿Qué es Proof of Work (PoW)?. (s.f.). Academy Bit2me. Recuperado de: <https://academy.bit2me.com/que-es-proof-of-work-pow/>. [17 de mayo de 2021]
- ¿Qué es un Algoritmo de Consenso?. (2018, 13 de diciembre). Academy Binance. Recuperado de: <https://academy.binance.com/es/articles/what-is-a-blockchain-consensus-algorithm#proof-of-work-pow>. [28 de mayo de 2021]
- ¿Qué es una quema de monedas? (2018, 9 de diciembre). Academy Binance. Recuperado de: <https://academy.binance.com/es/articles/what-is-a-coin-burn>. [10 de julio de 2021]
- ¿Qué es USDT(Tether)?.(s.f.). Academy Bit2me. Recuperado de: <https://academy.bit2me.com/que-es-usdt-theter-criptomoneda/> [11 de junio de 2021]
- ¿Qué son las DApps y por qué serán cada vez más importantes?. (2019, 22 de febrero). BBVA. Recuperado de: <https://www.bbva.com/es/que-son-las-dapps-y-porque-seran-cada-vez-mas-importantes/>. [16 de junio de 2021]
- ¿Qué son las ICO de criptomonedas?. (s.f.). Academy Bit2me. Recuperado de: <https://academy.bit2me.com/ico-criptomonedas/>. [17 de mayo de 2021]
- ¿Qué tipos de Blockchain o cadenas de bloques existen?. (2018, 8 de noviembre). Grupo Garatu It Solutions. Recuperado de: <https://grupogaratu.com/cuales-son-los-diferentes-tipos-de-blockchains-o-cadena-de-bloques/> [14 de junio de 2021]
- Quirós, F. (2020, 16 de julio). ¿Qué hace que Cardano tenga características diferentes a otras plataformas Blockchain?. *CoinTelegraph*. Recuperado de: <https://es.cointelegraph.com/news/what-makes-cardano-different-from-other-blockchain-platforms>[12 de mayo de 2021]
- Sáez, J. (2021, 1 de julio). ¿Qué son las DLT y en qué se diferencian de Blockchain?. *IEBS*. Recuperado de: <https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/>. [1 de julio de 2021]
- Solé, R. (2021, 19 de junio). Qué son los NFT y para qué sirven. *Profesional Review*. Recuperado de: <https://www.profesionalreview.com/2021/06/19/que-son-nft/>. [27 de mayo de 2021]